JOURNAL OF ALGEBRA 36, 364–394 (1975)

Characterizing Chevalley Groups of Rank Two and Characteristic Two by Their Sylow 2-Subgroups. I

GEOFFREY MASON*

University of California, Santa Cruz 95064

Received February 21, 1974

INTRODUCTION

In a recent paper [8], D. M. Goldschmidt has proved a very powerful and important theorem concerning 2-fusion in finite groups. What we are concerned with at this moment is not the actual statement of the result (we shall return to this in a later section) but rather one of its immediate corollaries, namely that the simple Chevalley groups of rank one and characteristic two are, with the exception of $A_1(4)$ and $A_1(8)$, characterized among the finite simple groups by their Sylow 2-subgroups. All of these simple groups have been characterized by their Sylow 2-subgroups previously ([3]. [12], [15], [21]), but Goldschmidt's result is the first to provide a unified approach to this problem.

The purpose of this paper is to point out the relevance of Goldschmidt's result to the characterization of Chevalley groups of characteristic two and rank bigger than one by their Sylow 2-subgroups. It obviously makes sense to begin with the Chevalley groups of rank two, namely A_2, ${}^2A_3$, ${}^2A_4$, B_2, G_2, ${}^3D_4$, and ${}^2F_4$ in the Chevalley notation. At this point we remark that Suzuki ([16], [17]) and Thomas ([18], [19], [20]) have characterized some of these groups by conditions placed on the centralizers of involutions, and moreover Collins [4] has recently characterized the simple Chevalley groups of type $A_2(2^n)$ by their Sylow 2-subgroups.

Before stating the main result of the present paper, we remind the reader of the following definition: if X is a finite group with Sylow 2-subgroup S, the group G is said to be *of type X* if a Sylow 2-subgroup of G is isomorphic to S. With this definition in mind, the main result of this paper is the following:

THEOREM A. *If G is a finite simple group of type $G_2(q)$, $q = 2^n \geqslant 4$, then $G \cong G_2(q)$.*

* Part of this research was done at the Mathematics Institute of the University of Warwick during the group theory year 1972–1973.

We remark that if G is a group of type $G_2(2)$ then G cannot be simple [5].

With regard to the problem of characterizing the other rank two Chevalley groups (of characteristic two) by their Sylow 2-subgroups, the proof of Theorem A should be thought of as a prototype. We hope to return to the remaining groups in later papers.

Before beginning the proof of Theorem A, we should like to consider the relevance of Theorem A to more general problems. Indeed, in the context of Gorenstein's programme for classifying the finite simple groups [10], the classification of such groups by their Sylow 2-subgroups appears (at the moment) to be relatively unimportant. Results like Theorem A merely provide temporary solace, in that no new simple groups arise. There is, however, another way in which one can view results like Theorem A which we would like to describe.

The Embedding Problem

Before stating the embedding problem, we will mention a few properties of the finite Chevalley groups which arise from the adjoint representation. Let $G^*(q)$ be such a group, where $q = p^r$ is a power of the prime p (we are not assuming that $p = 2$ here). Unless $G^*(q)$ is of Chevalley-type $A_1(2)$, $B_2(2)$, $G_2(2)$, or $A_1(3)$, $G^*(q)$ is a simple group. Let U be a Sylow p-subgroup of $G^*(q)$ with $B = N(U)$. If $G^*(q)$ has rank l then there are precisely 2^l subgroups of $G^*(q)$ which contain B, called the parabolic subgroups of $G^*(q)$. Moreover if P is a parabolic subgroup then $O_{p'}(P) = 1$.

Now let $G^*(q)$ and U be as above, and suppose that G_0 is a finite group satisfying the following

(a) $O_{p'}(G_0) = 1$,

(b) $O^{p'}(G_0) = G_0$,

(c) U_0 is a Sylow p-subgroup of G_0 and U_0 is isomorphic to U.

Then we will say that the group $G^*(q)$ admits an affirmative solution to the embedding problem if, for each such choice of G_0 and U_0, there is a parabolic subgroup P of $G^*(q)$ and an isomorphic embedding θ: $G_0 \to P$ such that the following diagram commutes:

$$\begin{tikzcd} G^*(q) & P \arrow[l] & U \arrow[l] \\ & G_0 \arrow[u, "\theta"] & U_0 \arrow[l] \arrow[u, "\cong"'] \end{tikzcd}$$

Here, all horizontal maps are the canonical embeddings.

Now it is certainly not the case that all adjoint Chevalley groups have an affirmative solution to the embedding problem. Indeed the groups $A_1(p^n)$ have elementary abelian Sylow p-subgroups and obviously are a counterexample. Less trivially, the group $A_4(2)$ has a Sylow 2-subgroup isomorphic to that of both the Mathieu group M_{24} and the sporadic group HTH originally found by Held [14], and if we let $G^*(q) = A_4(2)$ with $G_0 = M_{24}$ or HTH it is easy to check that θ does not exist. However, if $G^*(q)$ is not of Chevalley-type A_1, or A_2 and if $q > 2$ then counterexamples are harder to find.

In fact we will prove the following result.

THEOREM B. *The Chevalley group $G_2(q)$, $q = 2^n \geqslant 4$, admits an affirmative solution to the embedding problem.*

It is quite clear that Theorem B implies Theorem A. For if we choose the group G_0 to be simple the fact that all proper parabolic subgroups of $G^*(q)$ are nonsimple forces $P = G^*(q)$, so that θ is the required isomorphism. It turns out that we have to study the embedding problem for $G_2(2^n)$ in order to prove Theorem A, so that the proofs of both Theorem A and Theorem B are completed at essentially the same time. This is also the case in [4], where Collins shows that $A_2(q)$ has an affirmative solution so the embedding problem for $q = 2^n \geqslant 4$.

Now $G_2(q)$, $q = 2^n \geqslant 4$, has precisely four parabolic subgroups, that is subgroups containing $B = N(U)$ for U a Sylow 2-subgroup of $G_2(q)$. These are B, $G_2(q)$ itself, and two others which we denote by P_1 and P_2. For $i = 1, 2$ P_i is a 2-local subgroup with $O(P_i) = 1$, and setting $F_i = O_2(P_i)$, $O^{2'}(P_i)$ is a split extension of F_i by a group L_i isomorphic $SL(2, q)$. Next, suppose that G is an arbitrary finite group of type $G_2(q)$, $q = 2^n \geqslant 4$, with S a Sylow 2-subgroup of G. The idea of the proof of Theorems A and B is to study the groups $N_G(D)$ and $N_G(M)$, where D and M correspond to F_1 and F_2, respectively, under the isomorphism $U \cong S$. We will establish the following four results:

PROPOSITION 1.1. *Either $N_G(D)$ is solvable of 2-length one or else $N_G(D)/D \cdot O(N_G(D))$ is a* T.I.*-group in the sense of Suzuki* [17]. *Similarly, either $N_G(M)$ is solvable of 2-length one or $N_G(M)/MO(N_G(M))$ is a* T.I.*-group.*

PROPOSITION 1.2. *Suppose that $N_G(M)$ has 2-length one. Then $G = O(G) \cdot N_G(D)$.*

PROPOSITION 1.3. *Suppose that $N_G(D)$ has 2-length one, and $Y = Z(M)$. Then $G = O(G) \cdot N_G(Y)$.*

PROPOSITION 1.4. *Suppose that neither $N_G(M)$ nor $N_G(D)$ have 2-length one. Then $O^{2'}(G/O(G)) \cong G_2(q)$.*

It is quite clear that Theorem A is an immediate corollary of Propositions 1.2, 1.3, and 1.4. Once we have proved Proposition 1.1 it is a simple matter to completely describe the structure of $N_G(D)$ and $N_G(M)$, after which we take up the proofs of Propositions 1.2 and 1.3. These are based on the approach used in Section V of [18], and the idea is to construct certain abelian subgroups of S, which are strongly-closed in S with respect to G. Having done this Goldschmidt's result [8] enables us to conclude the proofs. Turning to the proof of Proposition 1.4, the idea is to construct the group $C_G(z)$ for z a central involution in S and show that it is isomorphic to the corresponding group in $G_2(q)$ (which we shall denote by $\mathscr{C}_q$). With the help of the first three propositions we are able to construct $C_G(z)$, but we can show only that it is isomorphic to an odd order extension of $\mathscr{C}_q$. At this point however, we can use a theorem of Harris [13] to complete the proof.

All of our notation is standard and, especially where the nomenclature for subgroups of G is concerned, follows that established in [18].

2. The Sylow 2-subgroup of $G_2(2^n)$

In this section we will describe the Sylow 2-subgroup S of the group $G_2(2^n)$. Almost all of this information can be found in [18] and is collected here for convenience and completeness sake.

Let $\Gamma = GF(q)$, $q = 2^n$, the finite field with 2^n elements. Then the group S can be described as follows: S is a product of six elementary abelian subgroups, $S = S_a S_b S_{a+b} S_{2a+b} S_{3a+b} S_{3a+2b}$. If we set $\Sigma^+ = \{a, b, a+b, 2a+b\ 3a+b, 3a+2b\}$, then for each $r \in \Sigma^+$ we can denote the elements of S_r by $\{x_r(\alpha) : \alpha \in \Gamma\}$. Each S_r is elementary abelian with multiplication $x_r(\alpha)x_r(\beta) = x_r(\alpha+\beta)$.

The product of any two elements of S can be determined by the following formula:

$$[x_a(\alpha), x_b(\beta)] = x_{a+b}(\alpha\beta)\, x_{2a+b}(\alpha^2\beta)\, x_{3a+b}(\alpha^3\beta), \tag{2.1}$$

$$[x_a(\alpha), x_{a+b}(\beta)] = x_{3a+b}(\alpha^2\beta)\, x_{3a+2b}(\alpha\beta^2), \tag{2.2}$$

$$[x_a(\alpha), x_{2a+b}(\beta)] = x_{3a+b}(\alpha\beta), \tag{2.3}$$

$$[x_b(\alpha), x_{3a+b}(\beta)] = x_{3a+2b}(\alpha\beta), \tag{2.4}$$

$$[x_{a+b}(\alpha), x_{2a+b}(\beta)] = x_{3+2b}(\alpha\beta), \tag{2.5}$$

$$[x_r(\alpha), x_s(\beta)] = 1 \quad \text{otherwise}$$

and the fact that each element x of S has a unique expression in the form $x = x_a(\alpha_1)\, x_b(\alpha_2)\, x_{a+b}(\alpha_3)\, x_{2a+b}(\alpha_4)\, x_{3a+b}(\alpha_5)\, x_{3a+2b}(\alpha_6)$.

All involutions of S have one of the following forms:

$$\begin{aligned}
&x_a(\alpha)\, x_{a+b}(\beta)\, x_{2a+b}(\alpha\beta)\, x_{3a+b}(\gamma)\, x_{3a+2b}(\delta), \quad \alpha \neq 0,\\
&x_b(\alpha)\, x_{a+b}(\beta)\, x_{2a+b}(\gamma)\, x_{3a+b}(\alpha\beta\gamma)\, x_{3a+2b}(\delta), \quad \alpha \neq 0,\\
&x_{a+b}(\alpha)\, x_{3a+b}(\beta)\, x_{3a+2b}(\gamma), \quad \alpha \neq 0,\\
&x_{2a+b}(\alpha)\, x_{3a+b}(\beta)\, x_{3a+2b}(\gamma), \quad \alpha \neq 0,\\
&x_{3a+b}(\alpha)\, x_{3a+2b}(\beta), \quad \alpha \neq 0,\\
&x_{3a+2b}(\alpha), \quad \alpha \neq 0.
\end{aligned}$$

We shall say that these involutions are of type (a), (b), $(a + b)$, $(2a + b)$, $(3a + b)$, or $(3a + 2b)$, respectively. These six types of involutions are conjugate in S to $x_a(\alpha)$, $x_b(\alpha)\, x_{2a+b}(\gamma + \alpha^{-1}\beta^2)$, $x_{a+b}(\alpha)$, $x_{2a+b}(\alpha)$, $x_{3a+b}(\alpha)$, and $x_{3a+2b}(\alpha)$, respectively, and the number of their conjugates in S is q^3, q^2, q^2, q^2, q, 1 respectively. S has order q^6. Each maximal elementary abelian subgroup of S has order q^3. There are five classes of such subgroups in S, with representatives $T = S_a S_{3a+b} S_{3a+2b}$, $U = S_b S_{2a+b} S_{3a+2b}$, $V = S_b S_{a+b} S_{3a+2b}$, $W = S_{2a+b} S_{3a+b} S_{3a+2b}$, $X = S_{a+b} S_{3a+b} S_{3a+2b}$. Of these, only W and X are normal in S, while the others each have q conjugates in S.

We set $Z = Z(S) = S_{3a+2b}$, $Y = Z_2(S) = S_{3a+b} S_{3a+2b}$. Finally, set $M = C_S(Y) = S_a S_{a+b} S_{2a+b} S_{3a+b} S_{3a+2b}$ and $D = S_b S_{a+b} S_{2a+b} S_{3a+b} S_{3a+2b}$. As noted in [18], M is characteristic in any Sylow 2-subgroup of G in which it is contained, as it is the unique subgroup of S of order q^5 with center of order q^2.

LEMMA 2.1. *S has an involutorial automorphism which interchanges W and X.*

Proof. See (6.24) of [18].

We also need the following technical result.

LEMMA 2.2. *Suppose that $x \in S - D$ and that $x^2 \in Z$. Then x is an involution.*

Proof. Suppose that $x = x_a(\alpha_1)\, x_b(\alpha_2)\, x_{a+b}(\alpha_3)\, x_{2a+b}(\alpha_4)\, x_{3a+b}(\alpha_5)\, x_{3a+2b}(\alpha_6)$. Because $x \notin D$ then $\alpha_1 \neq 0$. Using the formulae (2.1)–(2.5), we find that

$$\begin{aligned}
x^2 &= x_a(\alpha_1)\, x_b(\alpha_2)\, x_{a+b}(\alpha_3)\, x_{2a+b}(\alpha_4)\, x_{3a+b}(\alpha_5)\, x_a(\alpha_1)\\
&\quad \times x_b(\alpha_2)\, x_{a+b}(\alpha_3)\, x_{2a+b}(\alpha_4)\, x_{3a+b}(\alpha_5)\\
&\equiv x_a(\alpha_1)[x_b(\alpha_2), x_{3a+b}(\alpha_5)]\, x_{a+b}(\alpha_3)\, x_{2a+b}(\alpha_4)\, x_a(\alpha_1)\\
&\quad \times x_{a+b}(\alpha_1\alpha_2)\, x_{2a+b}(\alpha_1{}^2\alpha_2).\, x_{3a+b}(\alpha_1{}^3\alpha_2)\, x_{a+b}(\alpha_3)\, x_{2a+b}(\alpha_4)\\
&\equiv x_a(\alpha_1)\, [x_{a+b}(\alpha_3), x_{2a+b}(\alpha_4)]\, x_a(\alpha_1)\, x_{3a+b}(\alpha_1\alpha_4)\\
&\quad \times x_{3a+2b}(\alpha_1\alpha_3{}^2)\, x_{a+b}(\alpha_1\alpha_2)\, x_{2a+b}(\alpha_1{}^2\alpha_2)\, x_{3a+b}(\alpha_1{}^3\alpha_2)\\
&\equiv x_{a+b}(\alpha_1\alpha_2)\, x_{2a+b}(\alpha_1{}^2\alpha_2)\, x_{3a+b}(\alpha_1\alpha_4 + \alpha_1{}^2\alpha_3 + \alpha_1{}^3\alpha_2) \pmod{Z}.
\end{aligned}$$

Since $x^2 \in Z$, then uniqueness of expression forces $\alpha_1\alpha_2 = 0 = \alpha_1{}^2\alpha_2$, and also $\alpha_1\alpha_4 + \alpha_1{}^2\alpha_3 + \alpha_1{}^3\alpha_2 = 0$. As $\alpha_1 \neq 0$ then $\alpha_2 = 0$ and $\alpha_4 = \alpha_1\alpha_3$. Thus in fact $x = x_a(\alpha_1)\, x_{a+b}(\alpha_3)\, x_{2a+b}(\alpha_1\alpha_3)\, x_{3a+b}(\alpha_5)\, x_{3a+2b}(\alpha_6)$, and x is an involution of type (a), as required.

3. 2-Constrained Groups of Type $G_2(q)$, $q = 2^n \geqslant 4$

We recall that the group X is said to be 2-constrained if a Sylow 2-subgroup R of $O_{2',2}(X)$ satisfies $C_X(R) \leqslant O_{2',2}(X)$.

The first main result of this section is the following.

Proposition 3.1. *Suppose that G is an arbitrary 2-constrained group of type $G_2(q)$, $q = 2^n \geqslant 4$, with Sylow 2-subgroup S, and suppose further that $O(G) = 1$. Then $O_2(G) = D$, M, or S.*

Until further notice, G will be a group satisfying the hypotheses of Proposition 3.1. We shall prove Proposition 3.1 in a sequence of lemmas. We start with the following.

Lemma 3.1. *$Y \lhd G$ if, and only if, $M \lhd G$.*

Proof. If $M \lhd G$ then clearly $Y = Z(M) \lhd G$. Suppose conversely that $Y \lhd G$, then $C_G(Y) \lhd G$ and $O(C_G(Y)) = 1$. Now as G is 2-constrained then so also both $C_G(Y)$ and $C_G(Y)/Y$ are 2-constrained. But M is a S_2-subgroup of $C_G(Y)$ and M/Y a S_2-subgroup of $C_G(Y)/Y$. As M/Y is elementary abelian then $M/Y = O_2(C_G(Y)/Y)$, and hence $M \lhd G$, as required.

Lemma 3.2. *$Y < O_2(G)$.*

Proof. Set $N = O_2(G)$. Z is clearly contained in N by 2-constraint. First suppose that N contains an involution x which is of type (a), $(a + b)$ or $(2a + b)$. As all involutions of the coset $x.Y$ are conjugate in S it follows that $Y < x^S \leqslant N$, as required. Suppose that $Q = \Omega_1(N) \leqslant Y$. As $Q \lhd G$ we have that $C_G(Q)/Q$ is 2-constrained, and so $Y/Q \leqslant Z(O_2(C_G(Q)/Q)) < O_2(C_G(Q)/Q)$, from which the desired conclusion follows. Finally, we must consider the case that $\Omega_1(N)$ contains an involution x of type (b), but none of type (a), $(a + b)$ or $(2a + b)$. In this case we must have $Z = Z(\Omega_1(N))$ since by Eq. (2.4) we have $C_{S_{3a+b}}(x) = 1$. But then $Y/Z \leqslant Z(O_2(C_G(Z)/Z)) < O_2(C_G(Z)/Z)$, and again the desired containment follows.

From now on we will denote $O_2(G)$ by N. Next we prove

Lemma 3.3. *Suppose that $\Omega_1(N) \leqslant M$. Then either $N = W$, $N = X$, or $M = \Omega_1(N)$.*

Proof. By Lemma 3.2 we have $Y < N$. If $Y = \Omega_1(N)$, then $Y \lhd G$, so $M \lhd G$ by Lemma 3.1, a contradiction. Hence $Y < \Omega_1(N)$.

Next suppose that $Q = \Omega_1(N) \leqslant W$. As $Y < Q$ it follows from the commutator-formula that $W = C_S(Q)$ is a Sylow 2-subgroup of $C_G(Q) \lhd G$. Hence $W = O_2(C_G(Q)) = Q$. We will now show that $W = N$, so suppose this to be false. Thus there is an element $x \in N - W$, and we may take $x = x_a(\alpha_1)\, x_b(\alpha_2)\, x_{a+b}(\alpha_3)$. If $\alpha_1 = 0$ then x is an involution, which is nonsense, so $\alpha_1 \neq 0$. If $\alpha_2 = 0$, then N contains the element $y = x_a(\alpha_1) \times x_{a+b}(\alpha_3)\, x_{2a+b}(\alpha_1\alpha_3) \in \Omega_1(N) - W$. This is also a contradiction, so we can suppose that $\alpha_2 \neq 0$. In this case N contains the element x^2. An easy calculation shows that $x^2 \equiv x_{a+b}(\alpha_1\alpha_2) \pmod W$. As α_1, $\alpha_2 \neq 0$, then N contains $x_{a+b}(\alpha_1\alpha_2) \in \Omega_1(N) - W$, a contradiction. Thus we have shown that if $\Omega_1(N) \leqslant W$ then $N = W$. Similarly, if $\Omega_1(N) \leqslant X$ then $N = X$.

Suppose that $\Omega_1(N)$ is contained in neither W nor X. Then it is easy to see from the commutator formulae that $Y = Z(\Omega_1(N)) \lhd G$, and so $M \lhd G$ by Lemma 3.1. Thus Lemma 3.3 is proved.

LEMMA 3.4. *If $M = \Omega_1(N)$ then $M = N$.*

Proof. Otherwise $x = x_a(\alpha_1)\, x_b(\alpha_2) \cdots \in N - M$, so that $\alpha_2 \neq 0$. But then also $x_b(\alpha_2) \in N - M$, an impossibility as $x_b(\alpha_2)$ is an involution.

LEMMA 3.5. *Suppose that $\Omega_1(N) \nleqslant M$. Then either $N = D$ or $M \lhd G$.*

Proof. As $\Omega_1(N) \nleqslant M$ then N contains an involution x of type (b). Suppose that N also contains an involution of type (a). In this case we find that $Y = Z_2(\Omega_1(N)) \lhd G$ and so $M \lhd G$ by Lemma 3.1.

Hence we may assume that $\Omega_1(N) \leqslant D$. If $Z < Z(\Omega_1(N)) \lhd S$ we must have $Z(\Omega_1(N)) \cap S_{3a+b} \neq 1$. But $C_{S_{3a+b}}(x) = 1$ so this is impossible. Hence $Z = Z(\Omega_1(N)) \lhd G$ and $C_G(Z)/Z$ is 2-constrained. If $N \leqslant D$, the fact that D/Z is elementary abelian forces $D/Z = O_2(C_G(Z)/Z)$, and hence $D = N$ in this case. Finally, suppose that $N \nleqslant D$. Then there is an element $y = x_a(\alpha_1) \cdots \in N$ with $\alpha_1 \neq 0$. If we set $\bar{G} = G/Z$ it is easy to see that $\bar{Y} = C_{\bar{D}}(\bar{y})$. Thus we have $\bar{Y} = Z(\bar{N})$, $Y = Z_2(N) \lhd G$, and so $M \lhd G$ by Lemma 3.1.

LEMMA 3.6. *Suppose that $\Omega_1(N) \nleqslant M$ and $M \lhd G$. Then $N = S$.*

Proof. For under these conditions it is easy to see that $Z \lhd G$, $Y \lhd G$ and $WX = Z_3(S) \lhd G$. Let B be the stabilizer of the chain $M \rhd WX \rhd Y \rhd Z \rhd 1$ in G. Evidently S is a Sylow 2-subgroup of B and moreover $B \lhd G$. Suppose that P is a Sylow p-subgroup of B for p an odd prime. Then $[P, M] = 1$. But $C_G(Y) < G$ is a 2-constrained group with Sylow 2-subgroup M. It follows that $P \leqslant O(C_G(Y)) = 1$, and thus $B = S \lhd G$, as required.

Putting together the results of these first six lemmas, we have shown the following:

LEMMA 3.7. *N is one of the groups W, X, M, D or S.*

Before eliminating the first two possibilities, we prove the following.

LEMMA 3.8. *Either $N_G(M) = N_G(S)$, or $O^{2'}(N_G(M)/M) \cong SL(2, q)$.*

Proof. For suppose that $N_G(M)$ has two Sylow 2-subgroups S_1, S_2 such that $M < S_1 \cap S_2 = R$. As G is 2-constrained then so is $N_G(R)$, so by Lemma 3.7 we have $O_2(N_G(R)) = S_1 = S_2$. This proves that $N_G(M)/M$ is a T.I.-group with abelian Sylow 2-subgroups of order $q \geqslant 4$, so Lemma 3.8 follows from Suzuki's classification of such groups [17].

In the same way, we also obtain the following.

LEMMA 3.9. *Either $N_G(D) = N_G(S)$, or $O^{2'}(N_G(D)/D) \cong SL(2, q)$.*

LEMMA 3.10. *Suppose that $O^{2'}(N_G(D)/D) \cong SL(2, q)$. Then either $U \sim W$ and $V \sim X$, or $U \sim X$ and $V \sim W$ within $N_G(D)$. In particular, neither W nor X are normal in $N_G(D)$.*

Proof. The maximal elementary abelian subgroups of S contained in D are all conjugate in S to one of U, V, W, or X. Thus D contains $2q + 2$ such subgroups, namely the q conjugates of U and V, together with W and X. Each of these groups is normal in D, and so there is a permutation action of $O^{2'}(N_G(D)/D) \cong SL(2, q)$ on these $2q + 2$ subgroups. If $\mathscr{X}_1$ is the orbit of $SL(2, q)$ containing U, then $\mathscr{X}_1$ must contain at least the q S-conjugates of U, and similarly for the orbit $\mathscr{X}_2$ containing V. It follows that $|\mathscr{X}_1| = q$, $q + 1, q + 2, 2q, 2q + 1$, or $2q + 2$. As $q = 2^n \geqslant 4$ the only two possibilities are $|\mathscr{X}_1| = q + 1$ or $2q + 2$.

Suppose that $|\mathscr{X}_1| = 2q + 2$. In this case $W \sim X$ in G. As W and X are both normal in S it follows that we can choose $g \in G$ such that $W^g = X$ and $S^g = S$, that is $g \in N_G(S)$. But if $N(S) = SH$ with H a 2-complement of S in $N(S)$, H must fix both W and X as H has odd order and W and X are the only two normal abelian subgroups of S of order q^3. Thus $W \lhd N(S)$. As this fact contradicts the assumed existence of g, we are forced to conclude that $|\mathscr{X}_1| \neq 2q + 2$. It follows that $|\mathscr{X}_1| = |\mathscr{X}_2| = q + 1$, and Lemma 3.10 follows.

A similar analysis proves the following.

LEMMA 3.11. *Suppose that $O^{2'}(N_G(M)/M) \cong SL(2, q)$. Then either $T \sim W$ and $X \lhd N_G(M)$, or $T \sim X$ and $W \lhd N_G(M)$.*

LEMMA 3.12. *The two possibilities $N = W$ and $N = X$ are impossible.*

Proof. As the proofs of these two cases are entirely analogous we shall restrict our attention to the possibility that $N = W$. First we show that $W = S(G)$, the solvable radical of G. For otherwise, let $1 \neq Q$ be a Hall $2'$-subgroup of $O_{2',2}(G)$, so that $G = W \cdot N_G(Q)$. If we set $R = S_a \cdot W$ then $R = W \cdot N_R(Q)$. Set $R_1 = N_R(Q)$. Now $R_1 \cap W$ centralizes Q and $R_1/R_1 \cap W$ is elementary abelian, so if $1 = x_1, \ldots, x_s$ is a set of (right) coset representatives of $R_1 \cap W$ in R_1, we have $Q = \langle C_Q(x_i) : 2 \leqslant i \leqslant s \rangle$. Set $Q_i = C_Q(x_i)$ for $2 \leqslant i \leqslant s$.

Now $x_i \in R$, so $x_i = x_a(\alpha_i)w_i$ with $\alpha_i \in \Gamma$ and $w_i \in W$. Suppose that $\alpha_i = 0$. Then $x_i = w_i \in R_1 \cap W$, so $x_i = 1$ and $i = 1$. Thus for $i \geqslant 2$ we have $\alpha_i \neq 0$. Hence for $i \geqslant 2$, Q_i normalizes $C_W(x_i) = C_W(x_a(\alpha_i)) = Y$ as follows from Eq. (2.3). As $Q = \langle Q_i : i \geqslant 2 \rangle$ it follows that Q normalizes Y. By Lemma 3.1 we deduce that Q even normalizes M. Suppose that $N_G(M)$ has 2-length 1. Then Q normalizes S. According to Lemma 3.8 the only other possibility is that $O^{2'}(N_G(M)/M) \cong SL(2, q)$, in which case $[Q, S] < O^{2'}(N_G(M))$. But $S = W \cdot N_S(Q)$, and so $[Q, S] = [Q, W]$ $[Q, N_S(Q)] \leqslant W \cdot Q$. From this we find that $[QM/M, S/M] \leqslant QM/M$. As a Sylow 2-subgroup of $SL(2, q)$ normalizes no group of odd order for $q \geqslant 4$, we deduce that $[QM/M, S/M] = 1$, that is $[Q, S] \leqslant M$. So in either case Q normalizes S. But then $[Q, S] = [Q, W] \leqslant W$; as $W < \phi(S)$ it follows that Q centralizes S. Hence $Q \leqslant O(G) = 1$ as claimed.

Now the quotient group G/W is of type $L_3(q)$. Having shown that $W = S(G)$, it follows from a theorem of Collins [4] that $O^{2'}(G/W) \cong L_3(q)$. Set $\bar{G} = G/W$ with $\bar{L} = O^{2'}(\bar{G}) \cong L_3(q)$. From the structure of $L_3(q)$ we find that $O^{2'}(N_{\bar{L}}(\bar{D})/\bar{D}) \cong SL(2, q)$, and hence also $O^{2'}(N_G(D)/D) \cong SL(2, q)$. From Lemma 3.10 we find that $W \ntrianglelefteq N_G(D)$, which is ridiculous as we are supposing that $W \lhd G$. This completes the proof of Lemma 3.12.

To prove Proposition 1.1, observe that if G is any group of type $G_2(q)$, $q = 2^n$, then both $N_G(D)$ and $N_G(M)$ are 2-constrained. Thus Proposition 1.1 is an immediate consequence of Lemmas 3.8 and 3.9.

We prove two final results in this section which will be of use later on. Again, G is a 2-constrained group of type $G_2(q)$, $q = 2^n \geqslant 4$, $O(G) = 1$, and S is a Sylow 2-subgroup of G.

LEMMA 3.13. *Suppose that $O^{2'}(N_G(D)/D) \cong SL(2, q)$. Then $Z = Z(O^{2'}(N_G(D)))$ and moreover the extension $O^{2'}(N_G(D))/D$ splits.*

Proof. We certainly have $Z = Z(D)$. Now Z is elementary abelian of order q. As $SL(2, q)$ can only act trivially on such a group, it is clear that $Z = Z(O^{2'}(N_G(D)))$.

Now set $N = O^{2'}(N_G(D))$, so that $N/D \cong SL(2, q)$, and further set

$\bar{N} = N/Z$. Now $\bar{S} = S/Z$ is a Sylow 2-subgroup of $\bar{N}$, and moreover $\bar{D} \lhd \bar{S}$, $\bar{D}$ is elementary abelian and $\bar{D}$ is complemented in $\bar{S}$. By a theorem of Gaschutz [6] $\bar{D}$ is complemented in $\bar{N}$. Thus $\bar{N} = \overline{DL}$ and $\bar{D} \cap \bar{L} = 1$. Now $\bar{L}$ is a central extension of Z by $SL(2, q)$. Suppose that this extension splits: in this case D is clearly complemented in N and we are done. Suppose the extension does not split. In this case it is well-known that $q = 4$, that $L = Z_1 \times L_1$ with $L_1 \cong SL(2, 5)$ and Z_1 a subgroup of Z of index 2, and hence we have $N = DL_1$ with $D \cap L_1 = Z(L_1)$. In particular, $S = D(S \cap L_1)$ with $S \cap L_1$ a quaternion group. Choose $x \in (S \cap L_1) - Z(S \cap L_1)$. Then $x^2 \in Z$ and $x \in S - D$. By Lemma 2.2 we must have $x^2 = 1$. This is impossible, and so Lemma 3.13 follows.

LEMMA 3.14. *Suppose that $O^{2'}(N_G(M)/M) \cong SL(2, q)$. Then $O^{2'}(N_G(M))$ has a cyclic subgroup R of order $q + 1$ which acts frobeniusly on $Y = Z(M)$ (that is, $C_Y(x) = 1$ for $x \in R^{\#}$). In fact the set of conjugates $\{Z^x : x \in R^{\#}\}$ form a partition of Y.*

Proof. Set $N = O^{2'}(N_G(M))$ and $\bar{N} = N/M \cong SL(2, q)$. It is well-known that $\bar{N}$ has a cyclic subgroup $\bar{R}_0$ of order $q + 1$ which permutes the Sylow 2-subgroups of $\bar{N}$ cyclically. Now the inverse image R_0 of $\bar{R}_0$ has a 2-complement R, so that R is cyclic of order $q + 1$ and permutes the Sylow 2-subgroups of N cyclically.

Now suppose that some element $y \in Y - Z$ is conjugate in N to no element of Z, and let χ be the N-orbit containing y. Thus $|\chi| \leqslant q^2 - q$. As y is not a central involution then M is a Sylow 2-subgroup of $C_N(y)$, as so $|C_N(y)| = q^5 \cdot d$, where $d \mid q - 1$ or $d \mid q + 1$. Since $|N| = |\chi|$ $|C_N(y)|$ we deduce that $|\chi| = |N|/|C_N(y)| = q^6(q^2 - 1)/q^5 d \geqslant q^2 - q$. Hence in fact $|\chi| = q^2 - q$, so χ exhausts all elements of Y outside of Z and so $Z \lhd N$. As $SL(2, q)$ has no transitive representations of degree less that q (for $q = 2^n \geqslant 4$) then $Z \leqslant Z(N)$. But N acts on Y/Z which also has order q, so N acts trivially on Y/Z also. But then $N = O^{2'}(N)$ must centralize Y, which is nonsense. We have therefore shown that each $y \in Y - Z$ is conjugate to some element of Z, in other words Y is the union of the conjugates Z^n as n runs over N. Now $Z < N$ so $|N_N(Z)| = q^6(q - 1)$, as $N_N(Z) = N_N(Z) = N_N(S)$. Thus Z has exactly $|N : N_N(Z)| = q + 1$ conjugates in N, and the lemma follows easily.

4. The Degenerate Cases

In this section we will prove Propositions 1.2 and 1.3. As we have said before the approach is similar to that used in Section V of [18].

Throughout this section G is a group of type $G_2(q)$, $q = 2^n \geqslant 4$, with Sylow 2-subgroup S. To start with we assume the following.

HYPOTHESIS 4.1. $N_G(M)$ is solvable of 2-length 1.

LEMMA 4.1. *$N_G(W)$ and $N_G(X)$ are both solvable of 2-length 1.*

Proof. As both cases are very much the same, we will content ourselves with proving Lemma 4.1 for $N = N_G(W)$ only. Set $\bar{N} = N/O(N)$. Now as W is an element of $SCN(S)$ we certainly have that N, and hence also $\bar{N}$, is 2-constrained. By Proposition 3.1 it follows that $O_2(\bar{N})$ is either $\bar{D}$, $\bar{M}$, or $\bar{S}$. If $O_2(\bar{N}) = \bar{S}$ we are done. If $O_2(\bar{N}) = \bar{M}$ then $N = O(N)\, N_N(M)$.

But $N_N(M)$ has 2-length 1 by Hypothesis 4.1, so this case cannot occur. Finally, suppose that $O_2(\bar{N}) = \bar{D}$. Thus $N = O(N) \cdot N_N(D)$. Set $L = N_N(D)$, $\tilde{L} = L/O(L)$, so that L is 2-constrained. If L has 2-length 1 we arrive at a contradiction as before, so the only other possibility is that $O^{2'}(\tilde{L})/\tilde{D} \simeq SL(2, q)$. But as $\tilde{W} \lhd \tilde{T}$ this contradicts Lemma 3.10, and we are done.

LEMMA 4.2. *No element of $W - Z$ or $X - Z$ is conjugate to an element of Z.*

Proof. Again we will prove the result for elements of W, as the proof for X is the same. First suppose that $y \in Y - Z$ is conjugate to an element of Z. Thus a Sylow 2-subgroup S_1 of $C_G(y)$ is a Sylow 2-subgroup of G. Furthermore as $Y = Z(M)$ we can choose S_1 so that $M < S_1$. Now there is a $g \in G$ such that $y^g \in Z$ and $S_1^g = S$. By the uniqueness property of M mentioned in Section 2 we must have $M^g = M$. Now by Hypothesis 4.1, $N_G(M) = O(N_G(M))\, N_G(S)$, so we can assume without loss that $g \in N_G(S)$. But $Z \lhd N_G(S)$, so if $y \in Z$ then also $y^g \in Z$. We have shown that no element of $Y - Z$ is conjugate to an element of Z.

Suppose that $x \in W - Z$ is conjugate to an element of Z. Thus by the first paragraph we have $x \in W - Y$. Set $C = C_G(x)$ so that C contains a Sylow 2-subgroup S_1 of G. We may assume that $W < S_1$. Now $N_G(W)$ has 2-length 1 by Lemma 4.1, so $N(W) = O(N(W)) \cdot N(S)$. Thus $N_C(W) = O(N(W)) \cdot N_C(S)$. It follows that a Sylow 2-subgroup of $N_C(W)$ may be taken to be $C_S(x)$, which has order q^4. On the other hand, all maximal elementary abelian subgroups of S have order q^3 and normalizers of order at least q^5. Hence the same is true of S_1. In particular, $|N_{S_1}(W)| \geqslant q^5$, so Sylow 2-subgroups of $N_C(W)$ have order at least q^5. This is a contradiction, and the lemma is proved.

LEMMA 4.3. *$N_G(T)$ is solvable of 2-length 1, with M a Sylow 2-subgroup.*

Proof. Because $N(M)$ has 2-length 1, the fact that M is a Sylow 2-subgroup of $N(T)$ follows immediately from the fact that $M = N_S(T)$.

Since $T \in SCN(M)$ then $N = N_G(T)$ is certainly 2-constrained. Set $\bar{N} = N/O(N)$, and suppose to begin with that $\bar{T} \neq O_2(\bar{N})$. In this case the commutator relations (2.2) and (2.3) gives that $\bar{Y} = Z(O_2(\bar{N}))$, so $\bar{Y} \lhd \bar{N}$. But $\bar{Y} = Z(\bar{M})$ and $C_{\bar{N}}(\bar{Y})/\bar{Y}$ is 2-constrained with a trivial 2-regular core. As $\bar{M}/\bar{Y}$ is abelian it follows that $\bar{M}/\bar{Y} = O_2(C_{\bar{N}}(\bar{Y})/\bar{Y})$, and hence $\bar{M} \lhd \bar{N}$ in this case, as required.

So in proving 4.3, we may assume that $\bar{T} = O_2(\bar{N})$. We may also assume that $O^{2'}(\bar{N}) = \bar{N}$. Now by Walter's theorem classifying groups with abelian Sylow 2-subgroup [21] we find that $\tilde{\bar{N}} = \bar{N}/\bar{T}$ is a direct product $\tilde{\bar{X}}_1 \times \cdots \times \tilde{\bar{X}}_r$ of simple groups. Let $\bar{X}_1$ be the inverse image of $\tilde{\bar{X}}_1$ in $\bar{N}$, with $\bar{S}_1$ a Sylow 2-subgroup of $\bar{X}_1$. As $\bar{X}_1 \lhd \bar{N}$ then $\bar{N} = \bar{X}_1 \cdot N_{\bar{N}}(\bar{S}_1)$ by the Frattini argument. Now as $\bar{T} < \bar{S}_1 \lhd \bar{M}$ and $N_{\bar{N}}(\bar{S}_1)$ is 2-constrained with a trivial 2-regular core, the argument of the second paragraph proves that $\bar{M} \lhd N_{\bar{N}}(\bar{S}_1)$. It follows immediately that in fact $\tilde{\bar{N}} = \tilde{\bar{X}}_1$, so that $\tilde{\bar{N}} \cong SL(2, q^2)$, where we are again quoting Walter's theorem together with the fact that $| \bar{M} : \bar{T} | = q^2 \geqslant 16$. Thus $\tilde{\bar{N}}$ has a cyclic subgroup $\tilde{\bar{R}}$ of order $q^2 - 1$ acting transitively on the nonidentity elements of $\tilde{\bar{M}}$. Clearly $\bar{N}$ has a subgroup $\bar{R}_1$ with the same properties, and $\bar{R}_1$ normalizes $\bar{M}$. Thus $1 \neq \bar{R}_1 \leqslant N_{\bar{N}}(\bar{M}) = \overline{N_N(M)}$. If R_1 is the inverse image of $\bar{R}_1$ in N then $R_1 < N_N(M) \cdot O(N)$, and $R_1 = O(N) \cdot N_{R_1}(M)$. If we set $R_2 = N_{R_1}(M)$ then $R_2 < N_G(M) = O(N(M)) \cdot N(S)$ by Hypothesis 4.1. Now as we have seen before, $W \lhd N(S)$. Thus R_2 normalizes $O(N(M))W$ and R_1 normalizes $O(N)W$, and consequently $\bar{R}_1$ normalizes $\bar{W}$. But we have $\bar{T} < \overline{WT} < \bar{M}$, so in particular $\bar{R}_1$ cannot act transitively on $\bar{M}/\bar{T}$. This is a contradiction, and so we have shown that $\bar{N}$ must be solvable.

Thus as $\bar{N}/\bar{T}$ has elementary abelian S_2-subgroups then $\bar{N} = O_{2,2',2}(\bar{N})$. To show that $\bar{N}$ is 2-closed we proceed as in Lemma 3.12, so suppose that $1 \neq \bar{Q}$ is a Hall $2'$-subgroup of $O_{2,2'}(\bar{N})$. Then $\bar{N} = \bar{T}N_{\bar{N}}(\bar{Q})$ and if $R = TX_{2a+b}$ then $\bar{R} = \bar{T}N_{\bar{R}}(\bar{Q})$. Now the argument of Lemma 3.12 yields that $\bar{Y}$ is normalized by $\bar{Q}$. Thus $\bar{Y} \lhd \bar{N}$ and so also $\bar{M} = C_{\bar{N}}(\bar{Y}) \lhd \bar{N}$, as required. This completes the proof of Lemma 4.3. $O(N(M))W$ and R_1 normalizes $O(N)W$, and consequently $\bar{R}_1$ normalizes $\bar{W}$. But we have $\bar{T} < \overline{WT} < \bar{M}$, so in particular $\bar{R}_1$ cannot act transitively on $\bar{M}/\bar{T}$. This is a contradiction, and Lemma 4.3 follows.

LEMMA 4.4. *No element of $T - Z$ is conjugate to an element of Z.*

Proof. Because $N(T)$ has 2-length 1 by Lemma 4.3, the proof of Lemma 4.4 is precisely the same as in the second paragraph of the proof of Lemma 4.2, so we shall omit the details.

Lemma 4.5. *No element of $U - Z$ or $V - Z$ is conjugate to an element of Z.*

Proof. As the two cases are entirely analogous, we shall confine our attention to proof of the lemma for the group U only. First observe that $D = N_S(U)$. Suppose that U is conjugate to either W or X in G. By Lemma 4.2 both W and X have exactly $q - 1$ central involutions. Thus in this case the same is true of U, and the lemma is clear. Hence we may suppose that U is not conjugate to W or X, in which case D is a Sylow 2-subgroup of $N_G(U)$ and $N_G(U)$ is 2-constrained.

Next we show that $N_G(D)$ is solvable of 2-length 1. For if not, then $N_G(D)/D \cdot O(N(D))$ is a T.I.-group by Proposition 1.1; and furthermore it follows immediately from Lemma 3.10 that U is conjugate to one of W or X. As we are supposing that this is not the case, it follows that $N_G(D)$ is indeed solvable of 2-length 1.

Set $N = N_G(U)$ with $\bar{N} = N/O(N)$. If $\bar{U} \neq O_2(\bar{N})$ the commutator relations in S show that $\bar{Z} = [O_2(\bar{N}), O_2(\bar{N})] \lhd \bar{N}$. Because $\bar{D}/\bar{Z}$ is elementary abelian and because $C_{\bar{N}}(\bar{Z})/\bar{Z}$ is 2-constrained with a trivial 2-regular core, we find in this case that $\bar{D}/\bar{Z} = O_2(C_{\bar{N}}(\bar{Z})/\bar{Z})$ and hence $\bar{D} \lhd \bar{N}$, that is N has 2-length 1. Suppose that $\bar{U} = O_2(\bar{N})$. In this case we can repeat the argument used in paragraph 3 of Lemma 4.3 to obtain a contradiction, using the fact obtained above that $N_G(D)$ has 2-length 1.

Thus $N = N_G(U)$ has 2-length 1. So we are again in the position to obtain a contradiction as in Lemma 4.2. This completes the proof of Lemma 4.5.

Lemma 4.6. *Z is strongly closed in S with respect to G.*

Proof. This follows immediately from Lemmas 4.2, 4.4, and 4.5 since all involutions of S are conjugate in S to some involution of either T, U, V, W, or X.

Lemma 4.7. *$O(G)\, Z \lhd G$.*

Proof. We may assume that $O(G) = 1$ and try to prove that $Z \lhd G$. To do this we use the important result of Goldschmidt [8]. In the language of that paper Lemma 4.6 says that G is an $S(Z)$-group, so the main theorem of [8] tells us that G is an $S^*(Z)$-group.

Now set $K = Z^G \lhd G$. Because $O(G) = 1$ we also have $O(K) = 1$. Thus Goldschmidt's theorem tells us that K is a central product of an abelian 2-group and quasisimple groups of type I and II. Moreover quasisimple groups of type I are, by definition, perfect central extensions of the simple groups $L_2(2^n)$, $n \geqslant 3$, $Sz(2^{2n+1})$, $n \geqslant 1$, and $U_3(2^n)$, $n \geqslant 2$. Quasisimple groups L of type II are perfect central extensions of either $L_2(q)$, $q \equiv 3$ or $5 \pmod 8$ or a group of type JR, with $Z(L)$ of odd order. Using the fact that $O(K) = 1$ and that all of the Schur multipliers of the appropriate simple groups are known (we refer the reader to [11]), it is easy to see that the only possibility for a quasisimple normal subgroup L of K which is not actually simple is for L to be a perfect central extension of $Sz(8)$.

We will show that K is a 2-group, in which case we clearly have $K = Z \lhd G$, as required. So suppose first that K has a simple normal subgroup having an abelian Sylow 2-subgroup, and let A be the product of all such subgroups. Thus $1 \neq A \lhd G$ and a Sylow 2-subgroup $S_0 = A \cap S$ of A is elementary abelian. Suppose that $S_0 \leqslant Z = Z(S)$. Then S centralizes a Sylow 2-subgroup of each component of A, and hence S centralizes each component of A (or at least induces inner automorphisms of each such component) and so $S = S_0 \cdot C_S(A)$. As $S_0 \leqslant Z < \phi(S)$ then $S = C_S(A)$, which is ridiculous. Thus $S_0 \not\leqslant Z$. As $S_0 \lhd S$ then $Z < S_0$. Now $C_S(A) \lhd S$ and $S_0 \cap C_S(A) = 1$, and so $C_S(A) = 1$. Hence S acts faithfully on A. Now the same argument as above shows that no element of $S - S_0$ can act trivially on S_0, and so S_0 is self-centralizing in S. Thus S_0 is either W or X, and in particular $S_0 < \phi(S)$. Let H be a 2-complement to S_0 in $N_A(S_0)$. Then $SH = S_0$, $N_{SH}(H) = S_0HN_S(H)$, and $S = S_0N_S(H)$. This forces $S = N_S(H)$, yielding the contradiction that H centralizes S_0. We have proved that $A = 1$.

Now suppose that $1 \neq B$ is the product of all simple normal subgroups of K, set $S_0 = S \cap B$ and $T_0 = \Omega_1(S_0)$. After the result of the previous paragraph we may suppose that each component of B is isomorphic to some $Sz(2^{2n+1})$ or $U_3(2^n)$ for some appropriate n. In particular $T_0 = Z(S_0)$. As $S_0 \lhd S$ and S_0 is non-abelian we must have $Z < S_0$, and so in fact $Z \leqslant T_0$. This also implies that S acts faithfully on B. Suppose that there is an involution t of $S - T_0$ which centralizes T_0. Thus $t \in S - S_0$. It follows that t induces an inner automorphism of B, and so $C_S(B) \neq 1$, which is false. Hence we must have $T_0 = W$ or X, which is also impossible.

Assuming K is not a 2-group, we must have $K = F * C$, where $F = O_2(K) \leqslant Z$ and $1 \neq C$ is a central product of nontrivial perfect central extensions of $Sz(8)$. Set $S_0 = C \cap S$, a Sylow 2-subgroup of C. As $S_0 \lhd S$ we have $Z < S_0$ and thus $K = C$. Now it is well-known (c.f. Proposition 3(ii) of [3]) that S_0 has class 3, that $Z(S_0) = Z(C)$, and moreover Alperin and Gorenstein prove in [2] that $|Z(S_0)| \leqslant 4$. As $Z \leqslant Z(S_0)$ we deduce that $Z = Z(S_0)$ has order 4. Thus $q = 4$ and $|S| = 2^{12}$. As a Sylow 2-subgroup of $Sz(8)$ has order 2^6 it follows that $C/Z \cong Sz(8)$. Now $Sz(8)$ has no involutorial outer automorphisms, and it is easy to deduce that $C_S(C)$ properly contains Z. This is not the case, and so the proof of Lemma 4.7 is complete.

LEMMA 4.8. *D is strongly closed in S with respect to G.*

Proof. Choose $x \in T - Y$. We first prove that T is a Sylow 2-subgroup of $C_G(x)$. For if $N = N_G(T)$ then N is solvable of 2-length 1 by Lemma 4.3, with Sylow 2-subgroup M. Thus $N = O(N) \cdot N_N(M)$.

Let S_1 be a Sylow 2-subgroup of $C_G(x)$ which contains T. Then we have $T \leqslant N_{S_1}(T) \leqslant C(x) \cap N = O(N)\,(N_N(M) \cap C(x))$. But since $N_N(M)$ is 2-closed with Sylow 2-subgroup M then $C_M(x) = T$ is a Sylow 2-subgroup of $N_N(M) \cap C(x)$, and so $N_{S_1}(T) = T$. It follows that $S_1 = T$ as claimed.

Now suppose that some element $x \in S - D$ is conjugate to an element of D. As $O(G) \cdot Z \lhd G$ by Lemma 4.7, we can define $\bar{G} = G/O(G) \cdot Z$. Hence $\bar{x}$ is conjugate to an element of $\bar{D}$ in $\bar{G}$. As $\bar{D}$ is elementary abelian then $\bar{x}$ is an involution, that is $x^2 \in O(G) \cdot Z$. Thus in fact $x^2 \in Z$ and then Lemma 2.2 yields $x^2 = 1$. Hence x is an involution of type (a), so we can assume that $x = x_a(\alpha) \in T$ for some $\alpha \neq 0$. By the first paragraph a Sylow 2-subgroup of $C_G(x)$ has order q^3. But each involution of D has centralizer of order at least q^4 in S, so x cannot be conjugate to any such involution. This contradiction completes the proof of Lemma 4.8.

LEMMA 4.9. *$O(G)D \lhd G$. In particular, Proposition 1.2 is true.*

Proof. We can suppose that $O(G) = 1$ and try and prove that $D \lhd G$. By Lemma 4.7 we have $Z \lhd G$, so set $\bar{G} = G/Z$. By Lemma 4.8 $\bar{G}$ is an $S(\bar{D})$-group (observe that $\bar{D}$ is elementary abelian), so by the main result of [8] $\bar{G}$ is an $S^*(\bar{D})$-group also. Now we may assume without loss that $O^{2'}(G) = G$, in which case $Z = Z(G)$ and $O(\bar{G}) = 1$. Thus if $\bar{K} = \bar{D}^{\bar{G}}$, Goldschmidt's theorem tells us that $\bar{K}$ is a central product of an abelian 2-group and quasisimple groups of type I and II as described in Lemma 4.7.

First of all, let $\bar{A}$ be the product of all those simple normal subgroups $\bar{L}$ of $\bar{K}$ for which the extension $\bar{L} = L/Z$ splits. Then clearly A admits S and $A = Z \times A_0$, where A_0 is a direct product of simple groups. If $S_0 = S \cap A_0$ then $S_0 \lhd S$ and so $S_0 \cap Z \neq 1$. This is false unless $S_0 = 1$, and so $\bar{A} = 1$. Thus if $\bar{L}$ is a simple normal subgroup of $\bar{K}$ we must have $\bar{L} \cong L_2(q)$ for $q \equiv 3, 5 \pmod 8$ or $\bar{L} \cong Sz(8)$, and moreover the extension $\bar{L} = L/Z$ does not split. Suppose a component of the first kind exists. Then we must have $L = Z_0 \times L_0$ with $L_0 \cong SL_2(q)$, $q \equiv 3, 5 (8)$, and $1 \neq Z_0$ a subgroup of index 2 in Z. Suppose that $\langle z \rangle = Z \cap L_0$ and let $\bar{B}$ be the product of all of those components $\bar{L}$ with the property that $\langle z \rangle$ is the Frattini subgroup of a Sylow 2-group of the inverse image L of $\bar{L}$ in G. Then B admits S and $B = Z_0 \times B_0$ with B_0 a central product of copies of $SL(2, q)$'s, $q \equiv 3, 5 \pmod 8$. But then $B_0 \cap S \lhd S$ and $B_0 \cap S$ is a Sylow 2-subgroup of B_0. As B_0 is non-abelian then $Z < B_0 \cap S$, which is not the case. Thus $\bar{B} = 1$. Suppose that R has a component $\bar{L}$ of the second kind, i.e., $\bar{L} \cong Sz(8)$ and

L/Z does not split. If there is a "partial" splitting as in the last case the same argument yields a contradiction. So we can assume that L is a perfect central extension of Z by $Sz(8)$, in which case $|Z| = 4$ and $|S| = 2^{12}$. A consideration of orders now yields that $\bar{K} = O_2(\bar{K}) \times \bar{L}$. If $\bar{T}_0$ is a Sylow 2-subgroup of $\bar{L}$ then $|\Omega_1(\bar{T}_0)| = 2^3$. Now as $\bar{G}$ is an $S^*(\bar{D})$-group then $\bar{D} = O_2(\bar{K}) \times \Omega_1(\bar{T}_0)$ without loss, and so $|O_2(\bar{K})| = 2^5$ as $|\bar{D}| = 2^8$. But then a Sylow 2-subgroup of $\bar{K}$ has order 2^{11}, which is impossible.

Thus we have shown that $\bar{K}$ is a central product of $O_2(\bar{K})$ with certain nontrivial perfect central extensions of $Sz(8)$. Let $\bar{C}$ be the central product of all of those quasisimple components of $\bar{K}$. Because none of these components is simple, because $|Z| \geqslant 4$, and since the multiplier of $Sz(8)$ is a four-group [2], the central extensions of Z must split at least partially and so the argument of the last paragraph yields a contradiction. Hence $\bar{K} = O_2(\bar{K}) = \bar{D} \lhd \bar{G}$, and the lemma follows.

For the remainder of this section we will assume

Hypothesis 4.2. $N_G(D)$ is solvable of 2-length 1.

Lemma 4.10. *In proving proposition* 1.3, *we may assume that*

$$O^{2'}(N_G(M))/M \cdot O(N_G(M)) \cong SL(2, q).$$

Proof. For otherwise $N_G(M)$ is solvable of 2-length 1 by proposition 1.1. Thus Hypothesis 4.1 holds, and $G = O(G)\, N_G(D)$ by Proposition 1.2. Now Hypothesis 4.2 gives $G = O(G) \cdot N_G(S)$ and hence also $G = O(G)\, N_G(Y)$, as required.

From now on we will therefore suppose that $O^{2'}(N_G(M)/M \cdot O(N_G(M))) \cong SL(2, q)$. Lemma 3.11 tells us that exactly one of the two subgroups W, X is normal in $N_G(M)$. We shall denote by W_0 that one of W and X which is not normal in $N_G(M)$.

The proofs of Lemmas 4.1 and 4.2 are easily adapted to prove the following.

Lemma 4.11. $N_G(W_0)$ *is solvable of* 2-*length* 1. *Moreover no element of* $W_0 - Y$ *is conjugate to an element of* Y.

At this point we remark that by Lemma 3.14 all involutions of Y are central involutions (i.e., conjugate to an element of Z), hence the same is true of any involution conjugate to an involution of Y. This observation is used in the proof of Lemma 4.11 and some of the following lemmas.

Lemma 4.12. *No involution of* $U - Y$ *or* $V - Y$ *is conjugate to an element of* Y.

Proof. As both proofs are analogous we confine our attention to U. Indeed, as $U \lhd D$ and $N_G(D)$ has 2-length 1 by hypothesis, it is not difficult to see that $D = N_S(U)$ is a Sylow 2-subgroup of $N_G(U)$. The proof of Lemma 4.3 yields that $N_G(U)$ is solvable of 2-length 1, and then the proof of Lemma 4.2 suffices to obtain a contradiction if we assume that Lemma 4.12 is false.

LEMMA 4.13. *No element of $T - Y$ is conjugate to an element of Y.*

Proof. By Lemma 3.11 we have $T \sim W_0$, and the lemma follows from Lemma 4.11.

LEMMA 4.14. *$O(G) \cdot Y \lhd G$. In particular, Proposition 1.3 is true.*

Proof. We can assume that $O(G) = 1$ and try to prove that $Y \lhd G$. At any rate we have that Y is strongly closed in S with respect to G. For all involutions of $S - Y$ are conjugate in S to involutions of one of W_0, T, U or V, and so no element of Y is conjugate to an element of $S - Y$ by Lemmas 4.11, 4.12, and 4.13. As Y is abelian then G is an $S(Y)$-group, and thereby also an $S^*(Y)$-group by Goldschmidt's theorem. Finally, we may prove that $Y \lhd G$ is in precisely the same way that was used to prove $Z \lhd G$ in Lemma 4.7, so we may safely leave the proof of Lemma 4.14 at this point.

5. THE PROOF OF PROPOSITION 1.4

In this section we will prove that Proposition 1.4 holds, after which the Theorem A will also be proved. Thus from now on G is a group of type $G_2(q)$, $q = 2^n \geqslant 4$ satisfying the hypotheses of Proposition 1.4. In trying to prove Proposition 1.4 we may, and shall, assume that $O(G) = 1$ and $O^{2'}(G) = G$, and try to prove that $G \cong G_2(q)$.

Let S be a Sylow 2-subgroup of G with $Z = Z(S)$, and fix an involution $z \in Z^\#$. Set $C = C_G(z)$. As we have said before, our task is to prove that $C \cong \mathscr{C}_q$, the centralizer of a central involution in $G_2(q)$.

LEMMA 5.1. *The group $Q = \langle O(C_G(y)) : y \in Y^\# \rangle = \langle O(C_G(x)) : x \in Z^\# \rangle$, and furthermore Q has odd order.*

Proof. First consider the group C: C is a group of type $G_2(q)$, and $N_C(M)$ is 2-constrained. By Lemma 3.14 we see that $N_C(M)/M \cdot O(N_C(M))$ cannot be a T.I.-group as $N_C(M)/O(N_C(M))$ has a nontrivial center, so $N_C(M)$ satisfies Hypothesis 4.1. By Proposition 1.2 we have $C = O(C) \cdot N_C(D)$, and in particular C is 2-constrained. Now as z is an arbitrary element of Z, it follows from Lemma 3.14 that $C_G(y)$ is 2-constrained for all $y \in Y$.

It follows from this (c.f. Section 3.1 of [9]) that 0 is a Y-signalizer functor in the sense of [7]. By the main result of that paper, applicable since $m(Y) \geqslant 4$, we have that $Q = \langle O(C_G(y)) : y \in Y^{\#} \rangle$ has odd order.

Finally, it is trivial that $\langle O(C(x)) : x \in Z^{\#} \rangle \leqslant Q$. On the other hand, as Q has odd order and admits Z then $Q = \langle C_Q(x) \colon x \in Z^{\#} \rangle$. Since $C_Q(x)$ admits S and $C_G(x)$ is 2-constrained then $C_Q(x) \leqslant O(C_G(x))$, and hence $Q \leqslant \langle O(C_G(x) \colon x \in Z^{\#} \rangle$, as required.

LEMMA 5.2. $Q = 1$.

Proof. Suppose false. Then $Q \neq 1$. Set $N = N_G(Q)$. As Q has odd order and $O(G) = 1$ then N is a proper subgroup of G. Moreover it is clear from the description of Q given in Lemma 5.1 that N contains both $N_G(M)$ and $N_G(D)$. Thus N satisfies the hypotheses of Proposition 1.4. Proceeding inductively, we can assume that N satisfies the conclusions of Proposition 1.4. Hence $O^{2'}(N/Q) \cong G_2(q)$.

Now $G_2(q)$ has exactly two classes of involutions, so G has at most two classes of involutions. Suppose G has one class of involutions. Then the centralizers of all involutions are 2-constrained, so by the "balanced theorem" (cf. Section 4 of [9]) applicable since $SCN_3(S) \neq \varnothing$, we find that S normalizes no nontrivial groups of odd order. In particular $Q = 1$, as required. So we can suppose that G has two classes of involutions. In any case, since $O^{2'}(N/Q) \cong G_2(q)$ and N contains C, $N_G(D)$, and $N_G(M)$, these latter three groups are isomorphic to their counterparts in $G_2(q)$, modulo the possibility of normal subgroups of odd order and odd index. Thus we are in "essentially" the same position which Thomas arrives at in Section VIII of [18]. Thomas proves that the centralizer of a suitable noncentral involution is contained in $N_G(M)$. In our slightly more general situation, this is to be understood as proving that such a centralizer is (at least) 2-constrained. So in any case the "balanced theorem" is applicable and so $Q = 1$.

It follows from Lemma 5.2 that $O(N_G(D)) = 1$. So if we set $N = O^{2'}(N_G(D))$ then by Lemma 3.13 we know that N is a semidirect product $N = DL$ with $L \cong SL(2, q)$.

We must now set about proving the following.

PROPOSITION 5.1. *$N \cong \mathscr{C}_q$, the centralizer of a central involution in $G_2(q)$.*

We shall retain the notation established in the lines prior to the statement of Proposition 5.1 throughout the remainder of this section. Now by Lemma 3.11 exactly one of the groups W and X is normal in $N_G(M)$. By Lemma 2.1 we may and shall suppose that $W \lhd N_G(M)$.

LEMMA 5.3. *All involutions of $T - Y$ and $X - Y$ are conjugate to $x_a(1)$.*

Proof. We have that $N = D \cdot L$ with $D \cap L = 1$, so $S = D(S \cap L)$ with $S \cap L$ elementary abelian. Moreover all involutions of $S \cap L$ are conjugate in L, as is well-known. Now if $x \in (S \cap L)^{\#}$, then x is clearly an involution of type (a), so $x = x_a(\alpha)d$ with $\alpha \neq 0$ and $d \in D$. Note also that $x \sim x_a(\alpha)$ in S. Now suppose that $y = x_a(\alpha)d_1$ is also an element of $S \cap L$. Then $xy = x_a(\alpha)\, dx_a(\alpha)d_1 = d^{-1}d_1 \in (S \cap L) \cap D = 1$, and so $d = d_1$ and $x = y$. Thus as $x = x_a(\alpha)d$ ranges over $(S \cap L)$, α ranges over the elements of Γ. Now it follows immediately that all elements of $T - Y$ are conjugate to $x_a(1)$.

Next, as we are assuming that $W \lhd N_G(M)$, Lemma 3.11 tells us that $T \sim X$ in $N_G(M)$. But $Y \lhd N_G(M)$, so if $T^g = X$ with $g \in N(M)$ then g maps of set of coset representatives of Y in T onto a set of coset representatives of Y in X. If $1 = x_1, \ldots, x_q$ is such a transversal for Y in T, then the elements x_i for $2 \leqslant i \leqslant q$ are all conjugate by the first paragraph. Finally, as all elements of $x_i^g Y$ are conjugate in S for $i \geqslant 2$, the lemma follows.

Lemma 5.4. *$x_a(1)$ is a noncentral involution of G.*

Proof. We must show that $x_a(1)$ is conjugate to no involution of Z, so suppose this to be false. In fact as $N = D \cdot L$, we may repeat the proof of the corresponding result (8.1) of [18], as long as we check that no two distinct conjugates of M in N have an intersection which is elementary abelian of order q^3. So suppose that M_0 is some N-conjugate of M with the property that $M \cap M_0$ is elementary abelian of order q^3. We certainly have $M \cap M_0 \leqslant M \cap D = WX$, so we must have $M \cap M_0 = W$ or X as these are the only two elementary abelian subgroups of WX of order q^3.

Now let S, S_0 be Sylow 2-subgroups of N containing M, M_0, respectively. As $SL(2, q)$ is 2-transitive on its Sylow 2-subgroups the same is true of N, so we can choose an involution $x \in L$ with $S^x = S_0$. Hence also $M^x = M_0$ by the uniqueness property of M, and so x normalizes $M \cap M_0$. Because $L = \langle S, x \rangle$ and $M \cap M_0 \lhd S$ we deduce that $M \cap M_0 \lhd N$, that is either W or X is normal in N. This contradicts lemma 3.10, and the result follows.

Lemma 5.5. *We have $V \sim W$ and $U \sim X$ within N.*

Proof. If the lemma is false, we must have $U \sim W$ and $V \sim X$ in N by Lemma 3.10, so suppose that this is the case. Let $x_1 = x_b(\alpha)\, x_{a+b}(\beta) \times x_{3a+2b}(\gamma)$, $\alpha \neq 0$, be a noncentral involution of V. Thus x_1 is conjugate to an element of $X - Y$, and so $x_1 \sim x_{a+b}(1)$ by Lemma 5.3. Now we also have $x_1 \sim x_b(\alpha)\, x_{2a+b}(\alpha^{-1}\beta^2) = x_2$ in S. Since x_2 is a noncentral involution of U and as $U \sim W$ by assumption, then we must have $x_2 \sim x_{2a+b}(\alpha_1)\, x_{3a+b}(\beta_1) \times x_{3a+2b}(\gamma)$, with $\alpha_1 \neq 0$. As this latter element is conjugate to $x_{2a+b}(\alpha_1)$ in S, it follows that $x_{a+b}(1) \sim x_{2a+b}(\alpha_1)$.

Now both of these involutions are noncentral, so their centralizers in G

have Sylow 2-subgroups of order q^4. Thus $XS_b = C_S(x_{a+b}(1))$ and $WS_b = C_S(x_{2a+b}(\alpha_1))$ are Sylow 2-subgroups of $C_G(x_{a+b}(1))$ and $C_G(x_{2a+b}(\alpha_1))$, respectively. Hence there is a $g \in G$ satisfying $x_{a+b}(1)^g = x_{2a+b}(\alpha_1)$ and $(XS_b)^g = WS_b$. Since $Z = (XS_b)' = (WS_b)'$ it follows that $g \in N_G(Z)$. Now $N_G(Z)$ satisfies Hypothesis 4.1 and so $D \lhd N_G(Z)$ by Lemma 4.9 in particular $g \in N_G(D)$. Now by assumption, the $N_G(D)$-conjugates of V are X and the groups V^s for $s \in S$. As $x_{a+b}(1) \in V$ we must also have $x_{2a+b}(\alpha_1) \in X \cup \{V^s\colon s \in S\}$. As $\alpha_1 \neq 0$ this is impossible, and so Lemma 5.5 is proved.

LEMMA 5.6. *All involutions of $W - Y$ are conjugate to $x_a(1)$.*

Proof. First we will show that the only central involutions of W are those contained in Y. For by Lemma 5.5 we have $V \sim W$ in N. Suppose that $W^g = V$ with $g \in N$, and set $V_0 = Y^g$. Clearly, $Z < V_0$, so let $1 = x_1, \ldots, x_q$ be a set of coset representatives of Z in V_0. Each x_i, $i \geqslant 2$, can be written in the form $x_i = x_b(\alpha_i)\, x_{a+b}(\beta_i)$. Suppose that $\alpha_i = \alpha_j$. Then we have $x_i x_j = x_b(\alpha_i)\, x_{a+b}(\beta_i)\, x_b(\alpha_j)\, x_{a+b}(\beta_j) = x_{a+b}(\beta_i + \beta_j) \in V_0$. Now all elements of V_0 are central, so with Lemma 5.3 we deduce that $x_{a+b}(\beta_i + \beta_j) = 0$. Thus $\beta_i = \beta_j$ and $x_i = x_j$, so $i = j$. Thus as $x_i = x_b(\alpha_i)\, x_{a+b}(\beta_i)$ runs over the set of coset representatives of Z in V_0 so α_i runs over the elements of Γ.

Now suppose that some element $w \in W - Y$ is a central involution. As all elements of wY are conjugate in S then all elements of wY are central involutions, hence the same is true of $(wY)^g = w^g V_0$. Now we have $w^g = x_b(\alpha)\, x_{a+b}(\beta)\, x_{3a+2b}(\gamma) \in V$ for some α, β, $\gamma \in \Gamma$, and moreover α and β are not both zero. If $\alpha = 0$ then $w \sim x_{a+b}(\beta)\, x_{3a+2b}(\gamma) \sim x_{a+b}(\beta) \neq 1$ which is noncentral by Lemma 5.3. This is a contradiction, so we may suppose that $\alpha \neq 0$. Now choose that value of i such that $\alpha_i = \alpha$ (we know such an i exists by the previous paragraph) and consider the element $w^g x_i$. This element lies in $w^g V_0$ and hence is a central involution. On the other hand $w^g x_i = x_b(\alpha)\, x_{a+b}(\beta)\, x_{3a+2b}(\gamma)\, x_b(\alpha_i)\, x_{a+b}(\beta_i) = x_{a+b}(\beta + \beta_i)\, x_{3a+2b}(\gamma)$ by choice of i. By Lemma 5.3 we deduce that $\beta = \beta_i$. But then $w^g = x_b(\alpha_i)\, x_{a+b}(\beta_i) \times x_{3a+b}(\gamma) = x_i x_{3a+2b}(\gamma)$ and hence is in $V_0 = Y^g$. Thus $w \in Y$, against our choice of w. The lemma is proved.

Now let $S \cap L = S_0{}^*$ so that $S_0{}^*$ is elementary abelian of order q and $S = DS_0{}^*$ with $D \cap S_0{}^* = 1$. Let R be a 2-complement of S in $N_N(S)$. Thus R is cyclic of order $q - 1$ and acts regularly on the nonidentity elements of $S_0{}^*$. Furthermore, L has an involution t which inverts R elementwise and there is an element $x^* \in S_0{}^*$ with the property that $(tx^*)^3 = 1$. We fix all of this notation for the balance of the paper, and begin the proof of Proposition 5.1.

As R normalizes S, it certainly fixes Z, W, X, and also Y. Now by Lemma 5.5 the only N-conjugates of U are X and $\{U^s\colon s \in S\}$. Hence R permutes the S-conjugates of U, so replacing R by a suitable conjugate of R in S if necessary we can suppose that R fixes U. Similarly R permutes the S-conjugates of T, as follows from Lemma 3.11. Now all S-conjugates of T are actually conjugate in D, and so some D-conjugate of R, say R_1, normalizes T. But clearly R_1 also normalizes Z, U, W, and X, hence we can suppose that $R = R_1$ normalizes T. First we show that R fixes S_{3a+b}.

Observe that R fixes $U \cap X = S_{2a+b}Z$. Thus if $R = \langle r \rangle$, the action of r on S can be described as follows:

$$\begin{aligned} x_{3a+2b}(\alpha) &\to x_{3a+2b}(\alpha), \\ x_{3a+b}(\alpha) &\to x_{3a+b}(E_5(\alpha))\, x_{3a+2b}(E_6(\alpha)), \\ x_{2a+b}(\alpha) &\to x_{2a+b}(D_4(\alpha))\, x_{3a+2b}(D_6(\alpha)), \\ x_{a+b}(\alpha) &\to x_{a+b}(C_3(\alpha))\, x_{3a+b}(C_5(\alpha)\, x_{3a+2b}(C_6(\alpha)), \\ x_b(\alpha) &\to x_b(B_2(\alpha))\, x_{2a+b}(B_4(\alpha))\, x_{3a+2b}(B_6(\alpha)), \\ x_a(\alpha) &\to x_a(A_1(\alpha))\, x_{3a+b}(A_5(\alpha))\, x_{3a+2b}(A_6(\alpha)). \end{aligned} \tag{5.1}$$

Now because r induces an automorphism of S we can transform the commutator identities (2.1)–(2.5) by r and obtain new identities involving the A_i's, B_i's C_i's, D_i's, and E_i's (these are additive functions defined on Γ). Solving these equations yields in particular the following results:

$$\begin{gathered} A_1(\alpha) = A_1(1)\alpha, \qquad B_2(\alpha) = B_2(1)\alpha, \qquad C_3(\alpha) = C_3(1)\alpha, \\ D_4(\alpha) = D_4(1)\alpha, \qquad E_5(\alpha) = E_5(1)\alpha, \qquad E_6(\alpha) = 0, \qquad C_5(\alpha) = C_5(1)\alpha \\ B_4(\alpha) = B_4(1)\alpha, \qquad A_1(1) = D_4(1)^2 = C_3(1)^{-2}, \\ B_2(1) = D_4(1)^{-3} = E_5(1)^{-1}, \qquad C_5(1) = A_1(1)\, B_4(1). \end{gathered} \tag{5.2}$$

We remark that the function A_1 B_2, C_3, D_4, and E_5 are all epimorphisms, hence in particular $C_3(1)$ and $E_5(1)$ are nonzero. The proof of these results is very simple (although somewhat tedious), and we shall content ourselves by proving that E_6 is identically zero. This will prove that R fixes S_{3a+b}, and suffices as an illustration of the method. Thus we transform Eq. (2.3) by r. We obtain

$$\begin{aligned} &[x_a(A_1(\alpha))\, x_{3a+b}(A_5(\alpha))\, x_{3a+2b}(A_6(\alpha)),\, x_{2a+b}(D_4(\beta)) \\ &\quad \times x_{3a+2b}(D_6(\beta))] = x_{3a+b}(E_5(\alpha\beta))\, x_{3a+2b}(E_6(\alpha\beta)). \end{aligned}$$

The left-hand side of this becomes

$$[x_a(A_1(\alpha)),\, x_{2a+b}(D_4(\beta))] = x_{3a+b}(A_1(\alpha)\, D_4(\beta))$$

by Eq. (2.3) again. Now uniqueness of expression in S allows us to conclude that $x_{3a+2b}(E_6(\alpha\beta)) = 1$ for all α, $\beta \in \Gamma$, and hence E_6 is identically zero, as required.

Now R fixes $T = S_a Y$ and also Y. By complete reducibility R fixes some complement $S_a{}^*$ of Y in T. Suppose that

$$S_a{}^* = \{x_a(\alpha)\, y(a, \alpha): \alpha \in \Gamma, y(a, \alpha) \in Y\},$$

and suppose further that $x_1 = x_a(\alpha_1)\, y(a, \alpha_1)$ and $x_2 = x_a(\alpha_2)\, y(a, \alpha_2)$ are two distinct elements of $S_a{}^*$. Then $1 \neq x_1 x_2 = x_a(\alpha_1 + \alpha_2)\, y(a, \alpha_1)\, y(a, \alpha_2)$ is an element of $S_a{}^*$. Thus $x_a(\alpha_1 + \alpha_2) \neq 1$, that is $\alpha_1 \neq \alpha_2$. It follows that α ranges over Γ as $x_a(\alpha)\, y(a, \alpha)$ ranges over $S_a{}^*$. Because R is transitive on $(S_a{}^*)^{\#}$, then $A_1(1)$ is necessarily a generator of the multiplicative group of Γ. As $D_4(1)^2 = A_1(1)$ from Eqs. (5.2) the same is also true of $D_4(1)$. It is convenient if we let $D_4(1) = \lambda$. Then Eqs. (5.2) become

$$\begin{aligned} &A_1(\alpha) = \lambda^2\alpha, \quad B_2(\alpha) = \lambda^{-3}\alpha, \quad C_3(\alpha) = \lambda^{-1}\alpha, \quad D_4(\alpha) + \lambda\alpha, \\ &E_5(\alpha) = \lambda^3\alpha, \quad E_6(\alpha) = 0, \quad C_5(\alpha) = \lambda^2 B_4(1)\alpha, \quad B_4(\alpha) = B_4(1)\alpha. \end{aligned} \tag{5.3}$$

To show that R fixes V is harder. At least, R fixes some S-conjugate of V, hence R fixes $V^{x_a(\alpha_0)}$ for some $\alpha_0 \in \Gamma$. We must show that $\alpha_0 = 0$. Now suppose that t fixes X. Then $X \lhd \langle S, t\rangle = N$, which is false. Thus t does not fix X. But as t inverts R then R fixes X^t, and we deduce from Lemma 5.5 that $X^t = U$. A similar argument shows that $W^t = V^{x_a(\alpha_0)}$ also.

By complete reducibility R fixes subgroups $S_b{}^*$, S_{a+b}^*, S_{2a+b}^* of S satisfying $U = S_b{}^* S_{2a+b} Z$, and $S_{2a+b}^* Z = S_{2a+b} Z$, $X = S_{a+b}^* Y$. From these equations, together with Lemmas 5.4 and 5.6, we deduce that without loss

$$S_{3a+b}^t = S_b{}^*, \qquad (S_{a+b}^*)^t = S_{2a+b}^* \tag{5.4}$$

and in any case we find that

$$V^{x_a(\alpha_0)} = W^t = S_b{}^* S_{a+b}^* Z.$$

As we know the action of $x_a(\alpha_0)$ on V, it is not hard to deduce that

$$\begin{aligned} S_b{}^* &= \{x_b(\alpha)\, x_{2a+b}(\alpha_0{}^2\alpha)\, z(b, \alpha): \alpha \text{ ranges over } \Gamma, z(b, \alpha) \in Z\}, \\ S_{a+b}^* &= \{x_{a+b}(\alpha)\, x_{3a+b}(\alpha_0{}^2\alpha)\, z(a+b, \alpha): \alpha \text{ ranges over } \Gamma, z(a+b, \alpha) \in Z\}. \end{aligned} \tag{5.5}$$

Thus the action of t on D can be defined via

$$t\colon \begin{aligned} x_{3a+b}(\alpha) &\to x_{3a+2b}(\alpha), \\ x_{3a+b}(\alpha) &\to x_b(H_2(\alpha))\, x_{2a+b}(\alpha_0{}^2 H_2(\alpha))\, x_{3a+b}(H_6(\alpha)), \\ x_{2a+b}(\alpha) &\to x_{a+b}(J_3(\alpha))\, x_{3a+b}(\alpha_0{}^2 J_3(\alpha))\, x_{3a+2b}(J_6(\alpha)), \\ x_{a+b}(\alpha) &\to x_b(K_2(\alpha))\, x_{2a+b}(K_4(\alpha))\, x_{3a+2b}(K_6(\alpha)), \\ x_b(\alpha) &\to x_{a+b}(L_3(\alpha))\, x_{3a+b}(L_5(\alpha))\, x_{3a+2b}(L_6(\alpha)). \end{aligned} \tag{5.6}$$

Here, as before, indexed capital letters are additive functions defined on Γ. Moreover H_2 and J_3 are epimorphisms.

Now we have defined $x^* \in S_0{}^*$ to be that involution of $S_0{}^*$ which satisfies $(tx^*)^3 = 1$. As $x^* \in D$ we have $x^* = x_a(\alpha_0) \cdot d^*$ for some $\alpha_0 \neq 0$ and $d^* \in D$. Now as $x_a(\alpha)\, d^*(\alpha)$ ranges over the elements of $S_0{}^*$, so α ranges over the elements of Γ. As R is regular on $(S_0{}^*)$ then some power of r, say r^n, is such that $(x^*)^{r^n} = x_a(1)d^{**}$ for some d^{**} in D. Since t is an involution subject only to the condition that it inverts R then, replacing t by t^{r^n} if necessary, we may suppose that

$$(tx^*)^3 = 1, \qquad x^* = x_a(1)d^*,\ d^* \in D. \tag{5.7}$$

Now the fact that $t^2 = 1$, when applied to Eqs. (5.6) yields eight identities involving H_2, J_3, K_1, K_4, L_3, and L_5 (those involving H_6, J_6, K_6, L_6 are not so rewarding at the present!). Moreover, the application of (5.7) to the element $x_{3a+b}(\alpha)$ yields another four identities involving the same six functions. These last four enable us to completely determine what these functions are. It turns out that

$$\begin{gathered} H_2(\alpha) = \alpha, \qquad J_3(\alpha) = \alpha, \qquad K_2(\alpha) = \alpha_0{}^2\alpha, \\ K_4(\alpha) = \alpha(1 + \alpha_0{}^4), \qquad L_3(\alpha) = \alpha_0{}^2\alpha, \qquad L_5(\alpha) = \alpha(1 + \alpha_0{}^4). \end{gathered} \tag{5.8}$$

Having got a "first approximation" to the actions of t and r on D, we can calculate the right-hand side of the equation $x_{3a+b}(\alpha)^{trtr} = x_{3a+b}(\alpha)$, which holds as $trtr = 1$. Equating the coefficient of x_{a+b} to zero, we obtain that

$$B_4(1) = \alpha_0{}^2(\lambda + \lambda^{-3}). \tag{5.9}$$

Thus the actions of r, t on D are as follows: as well as acting trivially on Z, we have

$$r:\ \begin{aligned} x_{3a+b}(\alpha) &\to x_{3a+b}(\lambda^3\alpha), \\ x_{2a+b}(\alpha) &\to x_{2a+b}(\lambda\alpha)\, x_{3a+2b}(D_6(\alpha)), \\ x_{a+b}(\alpha) &\to x_{a+b}(\lambda^{-1}\alpha)\, x_{3a+b}(\alpha_0{}^2(\lambda^3 + \lambda^{-1})\alpha)\, x_{3a+2b}(C_6(\alpha)), \\ x_b(\alpha) &\to x_b(\lambda^{-3}\alpha)\, x_{2a+b}(\alpha_0{}^2(\lambda + \lambda^{-3})\alpha)\, x_{3a+2b}(B_6(\alpha)), \\ x_a(\alpha) &\to x_a(\lambda^2\alpha)\, x_{3a+b}(A_5(\alpha))\, x_{3a+2b}(A_6(\alpha)), \end{aligned} \tag{5.10}$$

$$t:\ \begin{aligned} x_{3a+b}(\alpha) &\to x_b(\alpha)\, x_{2a+b}(\alpha_0{}^2\alpha)\, x_{3a+2b}(H_6(\alpha)), \\ x_{2a+b}(\alpha) &\to x_{a+b}(\alpha)\, x_{3a+b}(\alpha_0{}^2\alpha)\, x_{3a+2b}(J_6(\alpha)), \\ x_{a+b}(\alpha) &\to x_b(\alpha_0{}^2\alpha)\, x_{2a+b}(1 + \alpha_0{}^4)\alpha)\, x_{3a+2b}(K_6(\alpha)), \\ x_b(\alpha) &\to x_{a+b}(\alpha_0{}^2\alpha)\, x_{3a+b}(1 + \alpha_0{}^4)\alpha)\, x_{3a+2b}(L_6(\alpha)). \end{aligned} \tag{5.11}$$

Now the transformation of Eq. (2.1) yields

$$\lambda^{-1}\alpha\beta^2\alpha_0^2(\lambda + \lambda^{-3}) + A_5(\alpha)\lambda^{-3}\beta = D_6(\alpha^2\beta) + C_6(\alpha\beta), \tag{5.12}$$

(5.12) holding for all $\alpha, \beta \in \Gamma$.

The fact that $(tr)^2 = 1$ yields the equations

$$\begin{aligned} D_6(\lambda^{-1}\alpha) + J_6(\lambda^{-1}\alpha) &= J_6(\alpha) + C_6(\alpha), \\ D_6(\alpha_0^2\alpha) + B_6(\alpha) &= H_6(\alpha) + H_6(\lambda^{-3}\alpha), \end{aligned} \tag{5.13}$$

whilst the fact that $t^2 = 1$ yields

$$\begin{aligned} H_6(\alpha) + L_6(\alpha) &= J_6(\alpha_0^2\alpha), \\ J_6(\alpha) + K_6(\alpha) &= H_6(\alpha_0^2\alpha). \end{aligned} \tag{5.14}$$

Next we return to the element $x^* = x_a(1)d^*$ of Eq. (5.7). This is where we must differentiate between the cases $q = 4$ and $q \geqslant 8$.

Suppose that $S_0^* = \{x_a(\alpha)\, x_{a+b}(P_3(\alpha))\, x_{2a+b}(\alpha P_3(\alpha))\, y(\alpha)\colon\ y(\alpha) \in Y\}$. Because R fixes S_0^* we find easily using Eqs. (5.10) that P_3 satisfies the functional equation

$$\lambda^{-1}P_3(\alpha) = P_3(\lambda^2\alpha), \qquad \text{all} \quad \alpha \in \Gamma.$$

As λ generates the multiplicative group of Γ it is easy to see that this last equation becomes

$$P_3(0) = 0,\ P_3(\alpha) = \alpha^{-1/2}P_3(1), \qquad \text{all} \quad \alpha \in \Gamma - \{0\}. \tag{5.15}$$

Now P_3 is certainly additive on Γ. We make the claim:

(*) *If P_3 is an additive function defined on $\Gamma = GF(2^n)$ and which staisfies (5.15) then either P_3 is identically zero, or else $\Gamma = GF(4)$ and $P_3(1)$ can be chosen arbitrarily.*

Proof. Suppose that $\Gamma = GF(4)$. Then for all $0 \neq \alpha \in \Gamma$, we have $\alpha^{-1/2} = \alpha$, so (5.15) becomes $P_3(\alpha) = \alpha P_3(1)$, so if $P_3(1) = 0$ then $P_3(\alpha)$ is identically zero. If $P_3(1) \neq 0$ P_3 is obviously additive.

Now suppose that $\Gamma \neq GF(4)$. Thus $\lambda^3 \neq 1$. As P_3 is additive (5.15) yields $P_3(1)(\alpha^{-1/2} + \beta^{-1/2}) = (\alpha + \beta)^{-1/2}P_3(1)$. Assuming P_3 is not identically zero we have $P_3(1) \neq 0$, so $(\alpha^{-1/2} + \beta^{-1/2}) = (\alpha + \beta)^{-1/2}$ for all $\alpha, \beta \neq 0$, $\alpha \neq \beta$. Choose $\alpha = 1$. We obtain $1 + \beta^{-1/2} = (1 + \beta)^{-1/2}$, and hence $(1 + \beta) = (1 + \beta^{-1/2})^{-2} = [(1 + \beta^{-1/2})^2]^{-1} = (1 + \beta^{-1})^{-1}$. Consequently, we find that $(1 + \beta^{-1})\,(1 + \beta) = 1$, i.e., $\beta + \beta^{-1} + 1 = 0$, i.e., $\beta^2 + \beta + 1 = 0$ on multiplication by $\beta \neq 0$. Comparing these last equations gives $\beta^2 = \beta^{-1}$, that is $\beta^3 = 1$, and this holds for all $\beta \neq 1$ or 0. But $\lambda^3 \neq 1$, which is a contradiction. The proof of (*) is complete.

Until further notice we will assume the following.

HYPOTHESIS 5.1. $q \geqslant 8$.

Under Hypothesis (5.1), (*) tells us that $S_0^* < S_a Y = T$. In particular then, $x^* \in T$, so $x^* = x_a(1)\, x_{3a+b}(\gamma_0)\, x_{3a+2b}(\delta_0)$ for some γ_0, $\delta_0 \in \Gamma$. If now we compute the right-hand side of the equation $x_{2a+b}(\alpha) = x_{2a+b}(\alpha)(x^*t)^3$, we find that (using (5.14))

$$J_6(\alpha) = \alpha(\gamma_0 + \alpha\alpha_0^2). \tag{5.16}$$

The first equation of (5.13) yields, since J_6 is additive, that $J_6(\alpha(1 + \lambda^{-1})) = C_6(\alpha) + D_6(\lambda^{-1}\alpha)$, and using (5.16) gives

$$C_6(\alpha) + D_6(\lambda^{-1}\alpha) = \alpha(1 + \lambda^{-1})\,[\gamma_0 + \alpha_0^2\alpha(1 + \lambda^{-1})]. \tag{5.17}$$

Replacing α by $\lambda^{-1}\beta$ in (5.17) gives

$$C_6(\lambda^{-1}\beta) + D_6(\lambda^{-2}\beta) = \lambda^{-1}\beta(1 + \lambda^{-1})[\gamma_0 + \alpha_0^2\lambda^{-1}\beta(1 + \lambda^{-1})]. \tag{5.18}$$

Now set $\alpha = \lambda^{-1}$ in Eq. (5.12). We obtain

$$C_6(\lambda^{-1}\beta) + D_6(\lambda^{-2}\beta) = \lambda^{-2}\beta^2\alpha_0^2(\lambda + \lambda^{-3}) + A_5(\lambda^{-1})\lambda^{-3}\beta. \tag{5.19}$$

Now both (5.18) and (5.19) hold for all $\beta \in \Gamma$. Thus equating the coefficients of β^2 and β to zero in the polynomial in β which results on adding (5.18) and (5.19), we obtain for β^2 that

$$\alpha_0^2\lambda^{-2}(\lambda + \lambda^{-3}) + \alpha_0^2\lambda^{-2}(1 + \lambda^{-1})^2 = 0, \tag{5.20}$$

and for β that

$$\gamma_0\lambda^{-1}(1 + \lambda^{-1}) + A_5(\lambda^{-1})\lambda^{-3} = 0. \tag{5.21}$$

Now because $q \geqslant 8$ then $\lambda^3 \neq 1$. Thus it is easily checked that (5.20) forces

$$\alpha_0 = 0. \tag{5.22}$$

Equation (5.22) allows us to simplify (5.12), (5.13), and (5.16) and at the same time eliminate J_6. Setting $\alpha = 1$ and then $\beta = 1$ to get two equations from (5.12), we obtain finally

$$\begin{aligned} A_5(1)\lambda^{-3}\beta &= D_6(\beta) + C_6(\beta), \\ A_5(\alpha)\lambda^{-3} &= D_6(\alpha^2) + C_6(\alpha), \\ C_6(\alpha) + D_6(\lambda^{-1}\alpha) &= \gamma_0\alpha(1 + \lambda^{-1}). \end{aligned} \tag{5.23}$$

Eliminating C_6 and D_6 from the Eqs. (5.23) gives

$$A_5(\alpha) = \lambda^3\gamma_0\alpha(1 + \alpha) + A_5(1)(1 + \lambda^{-1})^{-1}\,\alpha(\alpha + \lambda^{-1}). \tag{5.24}$$

As A_5 is additive, we can set $\alpha + 1$ in place of α in (5.24), and find that

$$\begin{aligned}A_5(\alpha) + A_5(1) &= A_5(\alpha + 1)\\ &= \lambda^3\gamma_0(\alpha + 1)\alpha + A_5(1)(1 + \lambda^{-1})^{-1}(\alpha + 1)(\alpha + 1 + \lambda^{-1}).\end{aligned}$$

The left-hand side of this last equation is given by (5.24). We see that

$$A_5(1)(1 + \lambda^{-1})^{-1}(\alpha + 1)(\alpha + 1 + \lambda^{-1}) = A_5(1) + A_5(1)(1 + \lambda^{-1})^{-1}\alpha(\alpha + \lambda^{-1}).$$

This becomes

$$A_5(1)[(1 + \lambda^{-1})^{-1}(1 + \alpha^2 + \alpha + \lambda^{-1}\alpha)] = A_5(1) + A_5(1)(1 + \lambda^{-1})^{-1}\alpha(\alpha + \lambda^{-1}).$$

Multiplying by $(1 + \lambda^{-1})$ and collecting terms yields

$$A_5(1)[1 + \alpha^2 + \alpha + \lambda^{-1}\alpha + 1 + \lambda^{-1} + \alpha^2 + \alpha\lambda^{-1}] = 0.$$

As this holds for all α, then obviously $A_5(1) = 0$. Now (5.23) becomes

$$C_6(\alpha) = D_6(\alpha) = \gamma_0\alpha,\ A_5(\alpha) = \gamma_0\alpha(\alpha + 1)\lambda^3. \tag{5.25}$$

The actions of t and r are now given by (5.10), (5.11), (5.20), (5.25), (5.13), and (5.14). We find that

$$r:\ \begin{aligned}&x_{3a+b}(\alpha) \to x_{3a+b}(\lambda^3\alpha),\\ &x_{2a+b}(\alpha) \to X_{2a+b}(\lambda\alpha)\, x_{3a+2b}(\gamma_0\alpha),\\ &x_{a+b}(\alpha) \to x_{a+b}(\lambda^{-1}\alpha)\, x_{3a+2b}(\gamma_0\alpha),\\ &x_b(\alpha) \to x_b(\lambda^{-3}\alpha)\, x_{3a+2b}(B_6(\alpha)),\\ &x_a(\alpha) \to x_a(\lambda^2 a)\, x_{3a+b}(\gamma_0\alpha(\alpha + 1)\lambda^3)\, x_{3a+2b}(A_6(\alpha)),\end{aligned} \tag{5.26}$$

$$t:\ \begin{aligned}&x_{3a+b}(\alpha) \to x_b(\alpha)\, x_{3a+2b}(H_6(\alpha)),\\ &x_{2a+b}(\alpha) \to x_{a+b}(\alpha)\, x_{3a+2b}(\gamma_0\alpha),\\ &x_{a+b}(\alpha) \to x_{2a+b}(\alpha)\, x_{3a+2b}(\gamma_0\alpha),\\ &x_b(\alpha) \to x_{3a+b}(\alpha)\, x_{3a+2b}(L_6(\alpha)),\end{aligned} \tag{5.27}$$

where also

$$H_6(\alpha) = L_6(\alpha) = B_6(\alpha(1 + \lambda^{-3})^{-1}). \tag{5.28}$$

From (5.5) and (5.22) we find that $S_b{}^* = \{x_b(\alpha)\, z(b, \alpha)\colon \alpha$ ranges over Γ and $z(b, \alpha) \in Z\}$. Now it is trivial to verify that if we define a map θ_1 on S which acts trivially on each root subgroup of S except S_b, and is such that $x_b(\alpha) \to x_b(\alpha)z_\alpha$ for z_α any element of Z, then θ_1 is an automorphism of S.

Hence we can choose such a θ_1 satisfying $S_b\theta_1 = S_b{}^*$. So we may assume to begin with that $S_b = S_b{}^*$, in which case R fixes S_b and hence B_6 is identically zero. Thus H_6 and L_6 are also identically zero.

Now define additive functions L_6, M_6 on Γ such that

$$S_{a+b}^* = \{x_{a+b}(\alpha)\, x_{3a+2b}(L_6(\alpha)) \colon \alpha \text{ ranges over } \Gamma\},$$
$$S_{2a+b}^* = \{x_{2a+b}(\alpha)\, x_{3a+2b}(M_6(\alpha) \colon \alpha \text{ ranges over } \Gamma\}.$$

Because $(S_{a+b}^*)^t = S_{2a+b}^*$ we find that

$$L_6(\alpha) = M_6(\alpha) + \gamma_0\alpha. \tag{5.29}$$

Because R fixes S_{a+b}^*, S_{2a+b}^* we also obtain

$$L_6(\alpha) + \gamma_0\alpha = L_6(\lambda^{-1}\alpha),$$
$$M_6(\alpha) + \gamma_0\alpha = M_6(\lambda\alpha).$$

These equations yield

$$\begin{aligned} L_6(\alpha) &= \gamma_0\alpha(1 + \lambda^{-1})^{-1}, \\ M_6(\alpha) &= \gamma_0\alpha(1 + \lambda)^{-1}. \end{aligned} \tag{5.30}$$

Now (5.29) and 5.30) give immediately that $\gamma_0 = 0$. Finally, suppose that N_5, N_6 are additive functions satisfying

$$S_0{}^* = \{x_a(\alpha)\, x_{3a+b}(N_5(\alpha))\, x_{3a+b}(N_6(\alpha))\}.$$

Because R fixes $S_0{}^*$ we find easily enough that

$$\lambda^3 N_5(\alpha) = N_5(\lambda^2\alpha). \tag{5.31}$$

This equation transforms to become $N_5(\alpha) = \alpha^{3/2}N_5(1)$. It is easily seen that N_5 must be identically zero as it is additive, and so $S_0{}^* = \{x_a(\alpha)\, x_{3a+2b}(N_6(\alpha))\}$.

Now there is an automorphism θ_2 of S such that $x_a(\alpha) \to x_a(\alpha)\, x_{3a+2b}(N_6(\alpha))$ and θ_2 acts trivially on all other root subgroups of S. Hence $S_a\theta_2 = S_0{}^*$, and we can assume that R fixes S_a, that is A_6 is identically zero. We have shown that

$$\begin{aligned}
r\colon\ & x_{3a+b}(\alpha) \to x_{3a+b}(\lambda^3\alpha), \qquad x_{2a+b}(\alpha) \to x_{2a+b}(\lambda\alpha),\\
& x_{a+b}(\alpha) \to x_{a+b}(\lambda^{-1}\alpha), \qquad x_b(\alpha) \to x_b(\lambda^{-3}\alpha),\\
& x_a(\alpha) \to x_a(\lambda^2\alpha), \qquad x_{3a+2b}(\alpha) \to x_{3a+2b}(\alpha),\\
t\colon\ & x_{3a+b}(\alpha) \leftrightarrow x_b(\alpha), \qquad x_{2a+b}(\alpha) \leftrightarrow x_{a+b}(\alpha),\\
& x_{3a+2b}(\alpha) \leftrightarrow x_{3a+2b}(\alpha).
\end{aligned}$$

Now it is trivial to verify that $N \cong \mathscr{C}_q$. We refer the reader to Sections II and III of [18] for details. Hence we have proved Proposition 5.1 in case $q \geqslant 8$.

Proof of Proposition 1.4 *for* $q \geqslant 8$. We use our earlier notation, so that $C = C_G(z)$ with $z \in Z^{\#}$. By Lemma 5.2 we have $O(C) = 1$. The result of Lemma 3.14 proves that C satisfies Hypothesis 4.1, so by Lemma 4.9 we have that $D \lhd C$, that is $C \leqslant N_G(D)$. As Proposition 5.1 holds for $q \geqslant 8$ we know in particular that if $N = O^{2'}(N_G(D))$ then $Z = Z(N)$, so of course $N \leqslant C$, and $N = O^{2'}(C)$.

We have shown that C is an odd-ordered extension of $N \cong \mathscr{C}_q$. At this point we can quote the main theorem of a paper of Harris [13] mentioned before. Now as $N_G(M)$ does not have 2-length 1, Lemma 3.14 guarantees that G has no normal 2-group unequal to 1, so Harris result tells us that $O^{2'}(G) \cong G_2(q)$. As $G = O^{2'}(G)$ then $G \cong G_2(q)$, and we are done.

HYPOTHESIS 5.2: $q = 4$. All equations up until (5.15) were derived with no assumptions on q, save that $q \geqslant 4$ of course. As in the case $q \geqslant 8$ we wish to show that $S_0{}^* < S_a Y = T$, however this requires a little more work if $q = 4$. At least, if we set

$$S_0{}^* = \{x_a(\alpha)\, x_{a+b}(P_3(\alpha))\, x_{2a+b}(\alpha P_3(\alpha))\, x_{3a+b}(P_5(\alpha))\, x_{3a+2b}(P_6(\alpha))\},$$

we still have that (Eq. 5.15) holds. As $\Gamma = GF(4)$, this can be rewritten as

$$P_3(\alpha) = P_3(1) \cdot \alpha, \qquad \text{all} \quad \alpha \in \Gamma. \tag{5.32}$$

Since R fixes $S_0{}^*$, we also find that

$$\begin{aligned} P_5(\alpha\lambda) &= A_5(\alpha) + \alpha_0{}^2 P_3(1)\, \alpha\lambda, \\ P_6(\alpha\lambda) &= A_6(\alpha) + C_6(P_3(1)\alpha) + D_6(P_3(1)\alpha^2). \end{aligned} \tag{5.33}$$

Now, the element x^* of $S_0{}^*$ becomes $x^* = x_a(1)\, x_{a+b}(P_3(1))\, x_{2a+b}(P_3(1)) \times x_{3a+b}(P_5(1))\, x_{3a+2b}(P_6(1))$, and of course $(tx^*)^3 = 1$. Applying this last identity to the element $x_{2a+b}(\alpha)$ we find by equating the coefficients of x_{3a+2b}, that

$$J_6(\alpha) = P_5(1)\alpha + \alpha\alpha_0{}^2 P_3(1) + \alpha_0{}^2\alpha^2 + P_3(1)\alpha. \tag{5.34}$$

By solving (5.34) simultaneously with the first equation of (5.33), the first equation of (5.13), and (5.12), we find that $P_3(1)\, \alpha\lambda = 0$ for all $\alpha \in \Gamma$. Hence we have

$$P_3(1) = 0. \tag{5.35}$$

From (5.35) and the form of the elements of $S_0{}^*$, we indeed find that $S_0{}^* < T$. In fact $S_0{}^* = \{x_a(\alpha)\, x_{3a+b}(P_5(\alpha))\, x_{3a+2b}(P_6(\alpha))\}$, where

$$P_5(\alpha) = A_5(\lambda^2\alpha), \qquad P_6(\alpha) = A_6(\lambda^2\alpha), \tag{5.36}$$

as follows easily from (5.35) and (5.33).

Now if $S^*_{a+b} = \{x_{a+b}(\alpha)\, x_{3a+b}(\alpha_0{}^2\alpha)\, x_{3a+2b}(W(\alpha))\}$, it is easy to check that $W(\alpha) + C_6(\alpha) = W(\lambda^2\alpha)$. Hence $W(\alpha) = C_6(\lambda^2\alpha)$ and

$$S^*_{a+b} = \{x_{a+b}(\alpha)\, x_{3a+b}(\alpha_0{}^2\alpha)\, x_{3a+2b}(C_6(\lambda^2\alpha)). \tag{5.37}$$

Similarly we obtain

$$S^*_{2a+b} = \{x_{2a+b}(\alpha)\, x_{3a+2b}(D_6(\lambda\alpha))\}. \tag{5.38}$$

Finally then, define a map φ on S as follows.

$$\varphi \quad \begin{aligned} &x_{3a+2b}(\alpha) \to x_{3a+2b}(\alpha),\ x_{3a+b}(\alpha) \to x_{3a+b}(\alpha),\\ &x_{2a+b}(\alpha) \to x_{2a+b}(\alpha)\, x_{3a+2b}(D_6(\lambda\alpha)),\\ &x_{a+b}(\alpha) \to x_{a+b}(\alpha)\, x_{3a+b}(\alpha_0{}^2\alpha)\, x_{3a+2b}(C_6(\lambda^2\alpha)),\\ &x_b(\alpha) \to x_b(\alpha)\, x_{2a+b}(\alpha_0{}^2\alpha)\, z(b,\beta) \qquad \text{any} \quad z(b,\beta) \in Z,\\ &x_a(\alpha) \to x_a(\alpha)\, x_{3a+b}(P_5(\alpha))\, x_{3a+2b}(P_6(\alpha)). \end{aligned}$$

We claim that φ is an automorphism of S. In fact all the relations (2.1)–(2.5) are trivially satisfied, except perhaps (2.1), so we only need show that $[x_a(\alpha), x_b(\beta)]^\varphi = [x_a(\alpha)^\varphi, x_b(\beta)^\varphi]$. Indeed we have that

$$\begin{aligned} [x_a(\alpha), x_b(\beta)]^\varphi &= x_{a+b}(\alpha\beta)^\varphi\, x_{2a+b}(\alpha\beta)^\varphi\, x_{3a+b}(\alpha^3\beta)^\varphi \\ &= x_{a+b}(\alpha\beta)\, x_{3a+b}(\alpha_0{}^2\alpha\beta)\, x_{3a+2b}(C_6(\lambda^2\alpha\beta)) \\ &\quad \times x_{2a+b}(\alpha^2\beta)\, x_{3a+2b}(D_6(\lambda\alpha^2\beta))\, x_{3a+b}(\alpha^3\beta), \end{aligned}$$

whilst

$$\begin{aligned} [x_a(\alpha)^\varphi, x_b(\beta)^\varphi] &= [x_a(\alpha)\, x_{3a+b}(P_5(\alpha)), x_b(\beta)\, x_{2a+b}(\alpha_0{}^2\beta)] \\ &= [x_a(\alpha)\, x_{3a+b}(P_5(\alpha)), x_b(\beta)] \\ &\quad \times [x_a(\alpha)\, x_{3a+b}(P_5(\alpha)), x_{2a+b}(\alpha_0{}^2\beta)]^{x_b(\beta)} \\ &= x_{a+b}(\alpha\beta)\, x_{2a+b}(\alpha^2\beta)\, x_{3a+b}(\alpha^3\beta) \\ &\quad \times x_{3a+2b}(\beta P_5(\alpha)\, x_{3a+b}(\alpha\beta\alpha_0{}^2(\, x_{3a+2b}(\alpha\beta^2\alpha_0{}^2). \end{aligned}$$

Equating the arguments of the corresponding elements, we find that φ is an automorphism of S if, and only if,

$$C_6(\lambda^2\alpha\beta) + D_6(\lambda\alpha^2\beta) = \beta P_5(\alpha) + \alpha\beta^2\alpha_0{}^2. \tag{5.39}$$

Now replacing α by $\lambda^2\alpha$ in Eq. (5.12) we obtain

$$\alpha_0{}^2\alpha\beta^2 + A_5(\lambda^2\alpha)\beta = D_6(\lambda\alpha^2\beta) + C_6(\lambda^2\alpha\beta). \tag{5.40}$$

Comparing (5.39) and (5.40), we must show that $P_5(\alpha) = A_5(\lambda^2\alpha)$. This is the first equation of (5.36), so φ is as required.

Finally, φ is clearly such that $S_{a+b} \to S^*_{a+b}$, $S_{2a+b} \to S^*_{2a+b}$, $S_a \to S_a{}^*$, and we can choose the elements $z(b, \beta)$ occuring in $\varphi(x_b(\alpha))$ such that φ: $S_b \to S_b{}^*$. Thus we may assume that R fixes S_{a+b}, S_{2a+b}, S_a, S_b, in which case it is easy to see that in fact $N \simeq \mathscr{C}_q$ (alternatively, φ has an obvious extension to an isomorphism of N with $\mathscr{C}_q$). We again refer the reader to [18] for details.

Finally, the proof of Proposition 1.4 for the case $q = 4$ follows exactly as in Hypothesis 5.1. This completes the proof of the Theorem A of this paper.

6. The Embedding Problem for G_2

In this final section we will explain how to obtain the proof of Theorem B. As the details are very similar to those already given we will often omit proofs.

So let G be an arbitrary finite group of type $G_2(q)$, $q = 2^n \geqslant 4$, with S a Sylow 2-subgroup of G. And suppose further that $O(G) = 1$ and $O^{2'}(G) = G$. We must show that for some parabolic subgroup P of $G_2(q)$ there is an isomorphic embedding θ: $G \to P$.

Again we let $P_1 = N(F_1)$ and $P_2 = N(F_2)$ be the two nontrivial parabolic subgroups of $G_2(q)$, with $F_i = O_2(P_i)$ for $i = 1, 2$. We choose F_1 and F_2 so that they correspond to D and M, respectively, under the isomorphism $S \underset{\to}{\cong} U$, for U a Sylow 2-subgroup of $G_2(q)$.

First suppose that both $N_G(D)$ and $N_G(M)$ have 2-length one. Then Propositions 1.2, 1.3, and 1.4 yield that $O(G)S \lhd G$. Thus in this case $G = S$ and the required isomorphism is clear. Suppose that neither $N_G(D)$ nor $N_G(M)$ have 2-length one. Proposition 1.4 yields $G \simeq G_2(q)$.

Next, suppose that $N_G(M)$ has 2-length one but that $N_G(D)$ does not have 2-length one. Proposition 1.2 gives $G = N_G(D)$, and Lemma 3.9 gives $G/D \simeq SL(2, q)$. But then by Proposition 5.1 we have $G \simeq \mathscr{C}_q = O^{2'}(P_1)$, so the required isomorphism exists.

Finally, we must consider the case that $N_G(D)$ has 2-length one, but that $N_G(M)$ does not have 2-length one. By Proposition 1.3 we find that $G = N_G(Y)$. In fact by an analysis entirely similar to Lemmas 4.8 and 4.9 we find that $G = N_G(M)$, after which Lemma 3.8 yields $N_G(M)/M \simeq SL(2, q)$. We will next prove that this extension splits. By Lemma 3.11 we may assume that $W \lhd G$, so let $\bar{G} = G/W$. As $\bar{M}$ is complemented in $\bar{S}$ then $\bar{M}$ is complemented in $\bar{G}$ by Gaschutz' theorem, so $\bar{G} = \bar{M} \cdot \bar{L}$ with $\bar{M} \cap \bar{L} = 1$, and $G = ML$ with $M \cap L = W$. Let $S_0 = S \cap L$ be a Sylow 2-subgroup of L. If the element $x = x_a(\alpha_1)\, x_b(\alpha_2) \cdots$ lies in S_0, the fact that S_0 has exponent four forces either α_1 or α_2 (or both) to be 0. In particular, it follows that $S_0 < D$. As W is complemented in D then W is complemented in L, again by Gaschutz theorem, so $G = M \cdot L_0$ with $M \cap L_0 = 1$, as required. Lastly, we need to show that $G \simeq O^{2'}(P_2)$ in this last case. This follows the same general lines as those laid down in the proof of Proposition 5.1. It is actually a little easier as $W \lhd G$ in this case. We will omit the details, and finish the discussion of the proof of Theorem B at this point.

References

1. J. L. Alperin, Centralizers of belian normal subgroups of p-groups, *J. Algebra* **1** (1964), 110–113.
2. J. L. Alperin and D. Gorenstein, The multiplicators of certain simple groups, *Proc. Amer. Math. Soc.* **17** (1966), 515–519.
3. M. J. Collins, The characterization of the Suzuki groups by their Sylow 2-subgroups, *Math. Z.* **123** (1971), 32–48.
4. M. J. Collins, The characterization of the finite groups whose Sylow 2-subgroups are of type $L_3(q)$, q even, *J. Algebra* **25** (1973), 490–512.
5. D. Fong, Groups of small order II, to appear.
6. W. Gaschutz, Zur Erweiterungstheorie endlicher Gruppen, *J. Math.* **190** (1952), 93–107.
7. D. M. Goldschmidt, Solvable signalizer functors on finite groups, *J. Algebra* **21** (1973), 137–148.
8. D. M. Goldschmidt, 2-fusion in finite groups, to appear.
9. D. M. Gorenstein, Centralizers of involutions in finite simple groups, *in* "Finite Simple Groups, Proceedings of London Mathematical Society Conference," Academic Press, London, 1971.
10. D. Gorenstein, A programme for classifying the finite simple groups, lecture notes given at the University of Chicago 1972.
11. R. L. Griess, Jr., Schur multipliers of the known finite simple groups, *Bull. Amer. Math. Soc.* **78** (1972), 68–71.
12. R. L. Griess, Jr., The characterization of $U_3(2^n)$ by its Sylow 2-subgroup, *Trans. Amer. Math. Soc.* **175** (1973), 181–186.
13. M. E. Harris, A characterization of odd-order extensions of $G_2(2^n)$ by the centralizer of one central involution, *J. Algebra* **23** (1972), 291–309.
14. D. Held, The simple groups related to M_{24}, *J. Algebra* **13** (1969), 253–296.
15. R. Lyons, A characterization of the group $U_3(4)$, *Trans. Amer. Math. Soc.* **164** (1972), 371–387.
16. M. Suzuki, On the characterization of linear groups V, to appear.
17. M. Suzuki, Finite groups of even order in which Sylow 2-subgroups are independent, *Ann. Math.* **80** (1964), 58–77.
18. G. Thomas, A characterization of the groups $G_2(2^n)$, *J. Algebra* **13** (1969), 87–118.
19. G. Thomas, A characterization of the Steinberg groups ${}^2D_4(q^3)$, $q = 2^n$, *J. Algebra* **14** (1970), 373–385.
20. G. Thomas, A characterization of the unitary groups $PSU_5(q^2)$, $q = 2^n$, *J. Algebra* **14** (1970).
21. J. H. Walter, The characterization of finite groups with abelian Sylow 2-subgroups, *Ann. Math.* **89** (1969), 405–514.